CLARKSON LAW FIRM, P.C.
Ryan J. Clarkson (SBN 257074)
rclarkson@clarksonlawfirm.com
Yana Hart (SBN 306499)
yhart@clarksonlawfirm.com
Tiara Avaness (SBN 343928)
tavaness@clarksonlawfirm.com
Valter Malkhasyan (SBN 348491)
vmalkhasyan@clarksonlawfirm.com
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
Fax: (231) 788-4070

Counsel for Plaintiff and the Proposed Classes

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

C.M., individually, and on behalf of all others similarly situated,

Plaintiff,

vs.

MARINHEALTH MEDICAL GROUP, INC.

Defendant.

Case No.: 3:23-cv-04179

CLASS ACTION COMPLAINT

1. VIOLATION OF CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CAL. CIV. CODE SECTION 56, *et seq*.
2. VIOLATION OF CALIFORNIA INVASION OF PRIVACY ACT, CAL. PENAL CODE SECTION 630, *et seq.*
3. VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE SECTION 17200, *et seq*.
4. INVASION OF PRIVACY UNDER CALIFORNIA CONSTITUTION
5. INVASION OF PRIVACY - INTRUSION UPON SECLUSION
6. NEGLIGENCE
7. BREACH OF IMPLIED CONTRACT
8. LARCENY/RECEIPT OF STOLEN PROPERTY, VIOLATION OF CALIFORNIA PENAL CODE SECTION 496(a) and (c)
9. UNJUST ENRICHMENT

DEMAND FOR JURY TRIAL

Plaintiff C.M. ("**Plaintiff**"), individually and on behalf of all others similarly situated brings this action against Defendant MarinHealth Medical Group, Inc. (**"Defendant"** or "**MarinHealth**").

Plaintiff's allegations are based upon personal knowledge as to himself and his own acts, and upon information and belief as to all other matters based on the investigation conducted by and through Plaintiff's attorneys. Plaintiff believes that substantial additional evidentiary support will exist for the allegations set forth herein, after a reasonable opportunity for discovery.

INTRODUCTION

1. Defendant MarinHealth Medical Group, Inc. is an organization consisting of three major divisions—a hospital, foundation, and network of expert clinicians—offering a wide range of clinical services to patients in Northern California.

2. MarinHealth Medical Center (the "Hospital") is a full-service hospital comprised of expert clinicians and physicians who practice at MarinHealth clinics, including more than one hundred fifty (150) providers in twenty (20) locations throughout Northern California.[1]

3. MarinHealth Medical Network (the "Network") is in charge of providing access to a wide range of expert physicians and providers, as well as allowing patients to access their MyChart patient portals.[2]

4. MarinHealth Foundation (the "Foundation") is a 501(c)(3) non-profit organization responsible for all of MarinHealth's fundraising.[3]

5. Defendant has disregarded the privacy rights of millions of visitors to and users of their websites ("**Users**" or "**Class Members**") by intentionally, willfully, recklessly and/or negligently failing to implement adequate and reasonable measures to ensure that that Users' personally identifiable information ("**PII**") and protected health information ("**PHI**") (collectively, "**Private Information**") was safeguarded. Instead, Defendant allowed unauthorized third parties, including Meta Platforms, Inc. d/b/a Facebook ("**Facebook**") to intercept Users' clicks, communications on, and visits of Defendant's websites, including https://www.mymarinhealth.org/

[1] *Marin Health Medical Network,* MARINHEALTH, https://www.mymarinhealth.org/career-opportunities/marinhealth-medical-network/ (last visited Aug. 8, 2023).
[2] *Id.*
[3] *MarinHealth Foundation,* MARINHEALTH, https://www.mymarinhealth.org/foundation/ (last visited Aug. 8, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

(the "**Site**") and https://www.mymarinhealth.org/mychart (the "**Portal**") (collectively, the "**Web Properties**").

6. Unbeknownst to Users and without Users' authorization or informed consent, Defendant installed Facebook's Meta Pixel ("**Meta Pixel**" or "**Pixel**") and other third-party tracking technology, in its Web Properties in order to intercept and send Private Information to third parties such as Facebook and/or Google LLC.

7. These Pixels collect Users' confidential and private PHI—including but not limited to details about their medical conditions, treatments and providers sought, and appointments—and send it to Facebook without prior, informed consent. These Pixels are snippets of code that track Users as they navigate through a website—logging which pages they visit, each button they click, and what information they provide in online forms. More specifically, the Meta Pixel sends information to Facebook via scripts running in a person's internet browser so each data packet comes labeled with a specific internet protocol ("**IP**") address that can be used in combination with other data to identify an individual or household. Additionally, if the person has an active Facebook account, the IP address is paired with their personal unique Facebook ID ("**FID**"), which Facebook uses to identify that individual.

8. Plaintiff and Class Members who visited and used Defendant's Web Properties understandably thought they were communicating with only their trusted healthcare providers, and reasonably believed that their sensitive and private PHI would be guarded with the utmost care. In browsing Defendant's websites – be it to make an appointment, locate a doctor with a specific specialty, find sensitive information about their diagnosis, or investigate treatment for their diagnosis – Plaintiff and Class Members did not expect that every search (including exact words and phrases they typed into Defendant's website search bars), page visit, or even their access/interactions on Defendant's online portals would be intercepted, captured, or otherwise shared with Facebook in order to target Plaintiff and Class Members, in conscious disregard of their privacy rights.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

9. Defendant encouraged Plaintiff and Class Members to access and use various digital tools via their Web Properties to, among other things, receive healthcare services, to gain additional insights into its Users, improve its return on marketing dollars and, ultimately, increase its revenue.

10. In exchange for installing the Pixels, Facebook provides Defendant with analytics about the advertisements they have placed as well as tools to target people who have visited Defendant's Web Properties.

11. While the information captured and disclosed without permission may vary depending on the Pixel(s) embedded, these "data packets" can be extensive, transmitting, for example, not just the name of the physician and her field of medicine, but also the first name, last name, email address, phone number, zip code, and city of residence entered in the booking form. That data is linked to a specific IP address. The amalgamation of these data points and unique identifying information results in an egregious, unauthorized dissemination of highly sensitive Private Information unique to each individual User.

12. The Meta Pixel can track and log each page a user visits, what buttons they click, as well as specific information they input into a website. In addition, if the person is (or recently has) logged into Facebook when they visit a particular website when a Meta Pixel is installed, some browsers will attach third-party cookies—another tracking mechanism—that allow Facebook to link Pixel data to specific Facebook accounts.

13. Alarmingly, the use of Meta Pixels on Defendant's Web Properties tracks extremely sensitive PHI such as health conditions (e.g., diabetes), diagnoses (e.g., COVID-19 or breast cancer), procedures, test results, treatment status, the treating physician, allergies, and PII.

14. Plaintiff had his Private Information, including sensitive medical information, harvested by Facebook through the Meta Pixel tracking tool without his consent when he entered his information into Defendant's Web Properties, and continued to have his privacy violated when his Private Information was used to turn a profit by way of targeted advertising related to his respective medical conditions and treatments sought.

15. Defendant knew that by embedding the Meta Pixel—a proprietary tracking and advertising tool developed by Facebook—on its Web Properties, it was permitting Facebook to

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

collect and use Plaintiff's and Class Members' Private Information, including sensitive medical information.

16. Defendant (or any third parties) did not obtain Plaintiff's and Class Members' prior consent before sharing their sensitive, confidential communications and Private Information with third parties such as Facebook.

17. Defendant's actions constitute an extreme invasion of Plaintiff's and Class Members' right to privacy and violate federal and state statutory and common law as well as Defendant's own Privacy Policies that affirmatively and unequivocally state that any personal information provided to Defendant will remain secure and protected.[4]

18. As a result of Defendant's conduct, Plaintiff and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) lack of trust in communicating with doctors online; (iii) emotional distress and heightened concerns related to the release of Private Information to third parties; (iv) loss of the benefit of the bargain; (v) diminution of value of the Private Information; (vi) statutory damages and (vii) continued and ongoing risk to their Private Information. Plaintiff and Class Members have a substantial risk of future harm, and thus injury in fact, due to the continued and ongoing risk of misuse of their Private Information that was shared by Defendant with third parties.

19. Plaintiff seeks, on behalf of himself and a class of similarly situated persons, to remedy these harms and therefore assert the following statutory and common law claims against Defendant: (i) Violation of the California Confidentiality of Medical Information Act ("**CMIA**"), Cal. Civ. Code § 56, *et seq.*; (ii) Violation of the California Invasion of Privacy Act ("**CIPA**"), Cal. Penal Code § 630, *et seq.*; Violation of the California Wiretapping Laws, Cal. Penal Code § 631, *et seq.;* (iii) Violation of California's Unfair Competition Law ("**UCL**"), Cal. Bus. & Prof. Code § 17200, *et seq*. – Unlawful and Unfair Business Practices; (iv) Invasion of Privacy under the California Constitution; (v) Common Law Invasion of Privacy; (vi) Negligence; (vii) (ix) Common Law Breach of Implied Contract; (x) Violation of California Penal Code § 496, *et seq.* and (xi)

[4] MarinHealth's Privacy Policies (and other affirmative representations) represent to Users that it will not share Private Information for marketing purposes unless patients provide written permission. *See* https://www.mymarinhealth.org/privacy-policy/ (last visited Aug. 4, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Common Law Unjust Enrichment.

PARTIES

20. Plaintiff C.M. is and at all relevant times was, a California resident.

21. Defendant MarinHealth Medical Group, Inc. is a not-for-profit healthcare system that serves the residents of Marin County and the greater North Bay. MarinHealth is comprised of Marin Health Medical Center, the MarinHealth Network, and the MarinHealth Foundation. MarinHealth is incorporated in California with its principal place of business located at 250 Bon Air, Rd., Greenbrae, CA 94904.[5]

JURISDICTION & VENUE

22. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C § 1332(d), because the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, there are more than one hundred (100) putative class members defined below, and minimal diversity exists because a significant portion of putative class members are citizens of a state different from the citizenship of at least one Defendant.

23. Pursuant to 28 U.S.C. Section 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District. The California Plaintiff is a citizen of California, resides in this District, and used Defendant's Web Properties within this District. Moreover, Defendant received substantial compensation from offering healthcare services in this District, and Defendant made numerous misrepresentations which had a substantial effect in this District, including, but not limited to, representing that it will only disclose Private Information provided to it under certain circumstances, ***which do not*** include disclosure of Private Information for marketing purposes.

24. Defendant is subject to personal jurisdiction in California based upon sufficient minimum contacts which exist between Defendant and California. Defendant is incorporated in California, maintains its principal place of business in California, is authorized to conduct and is conducting business in California.

[5] *About Us,* MARINHEALTH, https://www.mymarinhealth.org/about-us/ (last visited Aug. 4, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

FACTUAL BACKGROUND

25. Investigative journalists have published several reports detailing the seemingly ubiquitous use of tracking technologies on hospitals', health care providers' and telehealth companies' digital properties to surreptitiously capture and to disclose their Users' Private Information. Specifically, and for example, The Markup reported that 33 of the largest 100 hospital systems in the country utilized the Meta Pixel to send Facebook a packet of data whenever a person clicked a button to schedule a doctor's appointment.[6] Estimates are that over 664 hospital systems and providers utilize some form of tracking technology on their digital properties.[7]

26. Entities collecting and disclosing Users' Private Information face significant legal exposure under the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"), which applies specifically to healthcare providers, health insurance providers and healthcare data clearinghouses.[8]

27. The HIPAA privacy rule sets forth policies to protect all individually identifiable health information that is held or transmitted.[9] This is information that can be used to identify, contact, or locate a single person or can be used with other sources to identify a single individual. When PII is used in conjunction with one's physical or mental health or condition, health care, or one's payment for that health care, it becomes PHI.

28. The unilateral disclosure of such Private Information is unquestionably a violation of HIPAA, among other statutory and common laws. And, while some hospitals and other disclosing

---

[6] Todd Feathers, *et al.*, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last visited Aug. 4, 2023).

[7] Dave Muoio & Annie Burky, *Advocate Aurora, WakeMed get served class action over Meta's alleged patient data mining,* FIERCE HEALTHCARE (November 4, 2022), https://www.fiercehealthcare.com/health-tech/report-third-top-hospitals-websites-collecting-patient-data-facebook (last visited Aug. 4, 2023).

[8] Alfred Ng & Simon Fondrie-Teitler, *This Children's Hospital Network Was Giving Kids' Information to Facebook*, THE MARKUP (June 21, 2022), https://themarkup.org/pixel-hunt/2022/06/21/this-childrens-hospital-network-was-giving-kids-information-to-facebook (stating that "[w]hen you are going to a covered entity's website, and you're entering information related to scheduling an appointment, including your actual name, and potentially other identifying characteristics related to your medical condition, there's a strong possibility that HIPAA is going to apply in those situations") (last visited Aug. 4, 2023).

[9] The HIPAA Privacy Rule protects all electronically protected health information a covered entity like Defendant "create[s], receive[s], maintain[s], or transmit[s]" in electronic form. *See* 45 C.F.R. § 160.103.

entities attempt to seek refuge in the argument that these third parties allegedly do not store this Private Information, that argument is unavailing as the violation lies in the unlawful transmission of that data. As the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) reminded entities regulated under HIPAA in its recently issued *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* bulletin:

> ***Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[10]

OCR makes it clear that information that is routinely collected by vendors on public-facing websites, apps and web-based assets may be PHI as well, including unique identifiers such as IP addresses, device IDs, or email addresses.[11]

Defendant's Method of Transmitting Plaintiff's & Class Members' Private Information via the Meta Pixel.

29. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each "client device" (such as computer, tablet, or smart phone) accesses web content through a web browser (*e.g.*, Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser and Microsoft's Edge browser).

30. Every website is hosted by a computer "server" that holds the website's contents and through which the entity in charge of the website exchanges communications with Internet users' client devices via web browsers.

31. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses,

[10] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,* U.S. DEP'T OF HEALTH AND HUM. SERVICES, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited Aug. 4, 2023) (emphasis added).

[11] *See id.*; *see also* Mason Fitch, *HHS Bulletin Raises HIPAA Risks for Online Tracking Vendors*, LAW360 (December 13, 2022), https://www.law360.com/articles/1557792/hhs-bulletin-raises-hipaa-risks-for-online-tracking-vendors?copied=1 (last visited Aug. 4, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

along with corresponding cookies:

- **HTTP Request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies.[12]

- **Cookies**: a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are "third-party cookies" which means they can store and communicate data when visiting one website to an entirely different website.[13]

- **HTTP Response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.[14]

32. A patient's HTTP Request essentially asks the Defendant's Website to retrieve certain information (such as a physician's "Book an Appointment" page), and the HTTP Response renders or loads the requested information in the form of "Markup" (the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's Website).

33. Every website is comprised of Markup and "Source Code." Source Code is a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

34. Source Code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's User. The Pixel incorporated by Defendant uses Source Code that does just that. The Pixel acts much like a traditional wiretap.

35. When patients visit Defendant's Web Properties via an HTTP Request to Defendant's server, that server sends an HTTP Response including the Markup that displays the Webpage visible to the User and Source Code, including Defendant's Pixel.

36. Thus, Defendant is, in essence, handing patients a tapped device and once the

[12] *An overview of HTTP*, MDN WEB DOCS, https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview (last visited Aug. 4, 2023).

[13] *HTTP cookies*, MDN WEB DOCS, https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies (last visited Aug. 4, 2023).

[14] *An overview of HTTP*, *supra* note 13. One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses. *HTTP Messages*, MDN WEB DOCS, https://developer.mozilla.org/en-US/docs/Web/HTTP/Messages (last visited Aug. 4, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Webpage is loaded into the User's browser, the software-based wiretap is quietly waiting for private communications on the Webpage to trigger the tap, which intercepts those communications—intended only for Defendant—and transmits those communications to third parties, including Facebook. Such conduct occurs on a continuous, and not sporadic, basis.

37. Third parties, like Facebook, place third-party cookies in the web browsers of Users logged into their services.

38. These cookies uniquely identify the User and are sent with each intercepted communication to ensure the third-party can uniquely identify the patient associated with the Private Information intercepted.

39. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. This is why third parties bent on gathering Private Information, like Facebook, implement workarounds that cannot be evaded by savvy users.

40. Facebook's workaround, for example, is called CAPI, which is an "effective" workaround because it does not intercept data communicated from the User's browser. Instead, CAPI "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]."[15]

41. Thus, the communications between patients and Defendant, which are necessary to use Defendant's Websites, are actually received by Defendant and stored on their server before CAPI collects and sends the Private Information contained in those communications directly from Defendant to Facebook.

42. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

43. While there is no way to confirm with certainty that a Web host like Defendant has implemented workarounds like CAPI without access to the host server, companies like Facebook instruct Defendant to "[u]se the CAPI in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendant "to share website events [with

[15] Michael Mata, *Stop Data Loss with Facebook Server-Side Tracking*, MADGICX (March 18, 2022), https://madgicx.com/blog/facebook-server-side-tracking (last visited Aug. 4, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Facebook] that the pixel may lose."[16]

44. The third parties to whom a website transmits data through Pixels and associated workarounds do not provide any substantive content relating to the User's communications. Instead, these third parties are typically procured to track User data and communications for marketing purposes of the website owner (i.e., to bolster profits).

45. Thus, without any knowledge, authorization, or action by a User, a website owner like Defendant can use its source code to commandeer the User's computing device, causing the device to contemporaneously and invisibly redirect the Users' communications to third parties.

46. In this case, Defendant employed the Tracking Pixel and CAPI to intercept, duplicate and re-direct Plaintiff's and Class Members' Private Information to Facebook.

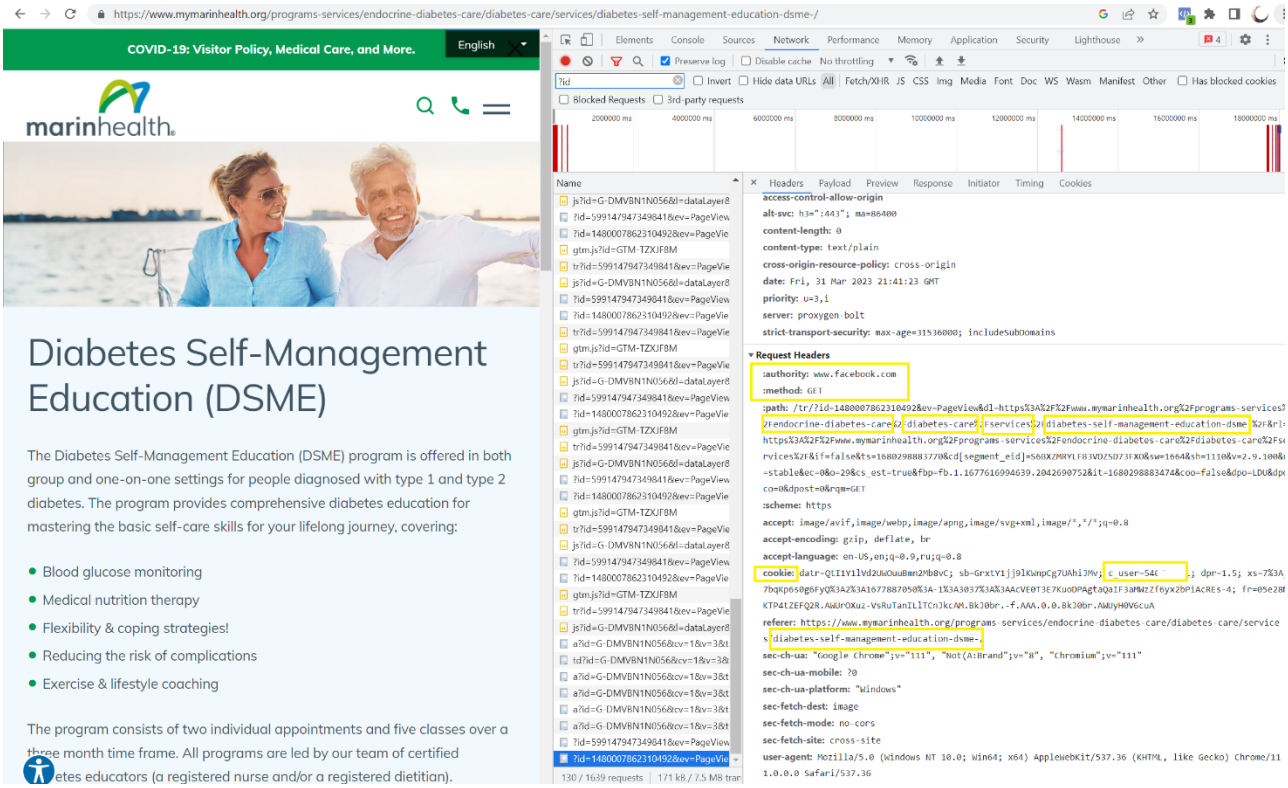
47. By way of example, MarinHealth shared with third parties Plaintiff's and Class Members' patient status, their medical conditions, the type of medical treatment or provider sought, names of specific providers, and the fact that the individual attempted to or did book a medical appointment. This Private Information was shared at the same time as certain HIPPA identifiers including patient's IP address, and along with their unique Facebook ID. Such information was shared without patient's express consent even though it allows a third party (*e.g.,* Facebook) to know that a specific patient was or is being treated for a specific type of medical condition.

48. For example, if a patient with diabetes researched their type of diabetes or looked up available care options when visiting www.mymarinhealth.org, including "Diabetes Self-management Education" program provided by Defendant, that information would have been shared with Facebook along with unique identifiers including the patient's Facebook ID. Someone seeking gender-affirming surgery would have had their sensitive and private information shared in the same manner (see ***Figure 1*** below).

[16] *See Best practices for Conversions API,* META, https://www.facebook.com/business/help/308855623839366?id=818859032317965 (last visited Aug. 4, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

***Figure 1**: Image from https://www.mymarinhealth.org/programs-services/endocrine-diabetes-care/diabetes-care/services/diabetes-self-management-education-dsme-/.*



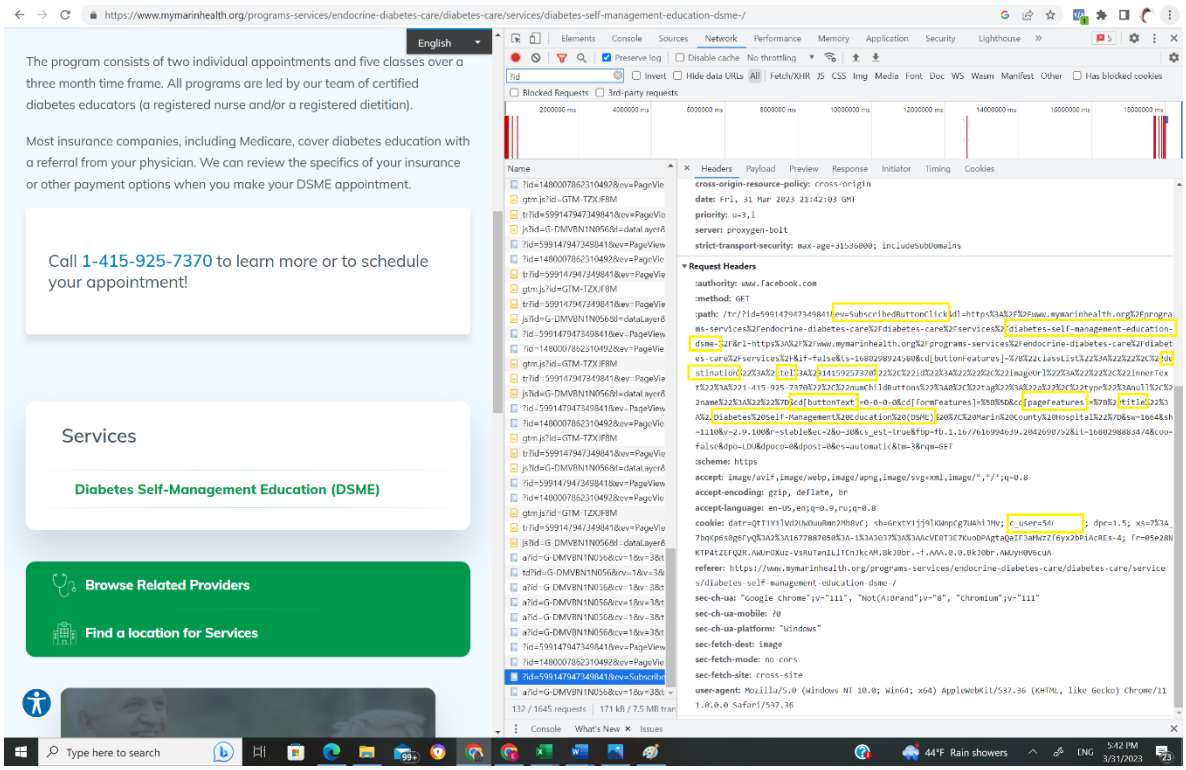
49. The patient visiting this particular web page only sees the Markup, not the Defendant's Source Code or underlying HTTP Requests and Responses. In reality, Defendant's Source Code and underlying HTTP Requests and Responses share the patient's personal information with Facebook, including the fact that the patient is looking for treatment for his Diabetes diagnosis along with the patient's unique Facebook identifiers.

50. Defendant provides an option to click a dedicated phone number to call its specialized programs for patients, including the Diabetes Self-Management Education program, to learn more or enroll. If a User diagnosed with diabetes clicks on the phone button, this information, including the name of the program and the phone number clicked, is also shared with Facebook, via the "SubscribedButtonClick" event (see ***Figure 2*** below)[17]:

[17] The image in Figure 2 was taken from https://www.mymarinhealth.org/programs-services/endocrine-diabetes-care/diabetes-care/services/diabetes-self-management-education-dsme-/ after a User of Defendant's Website clicked the phone number for the Diabetes Self-Management Education Program.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

***Figure 2**: Image from https://www.mymarinhealth.org/programs-services/endocrine-diabetes-care/diabetes-care/services/diabetes-self-management-education-dsme-/.*



51. Similarly, if a User searches for "prostate cancer treatment options" on Defendant's Website, Defendant shares that information with Facebook, along with the User's personal identifiers:

///

///

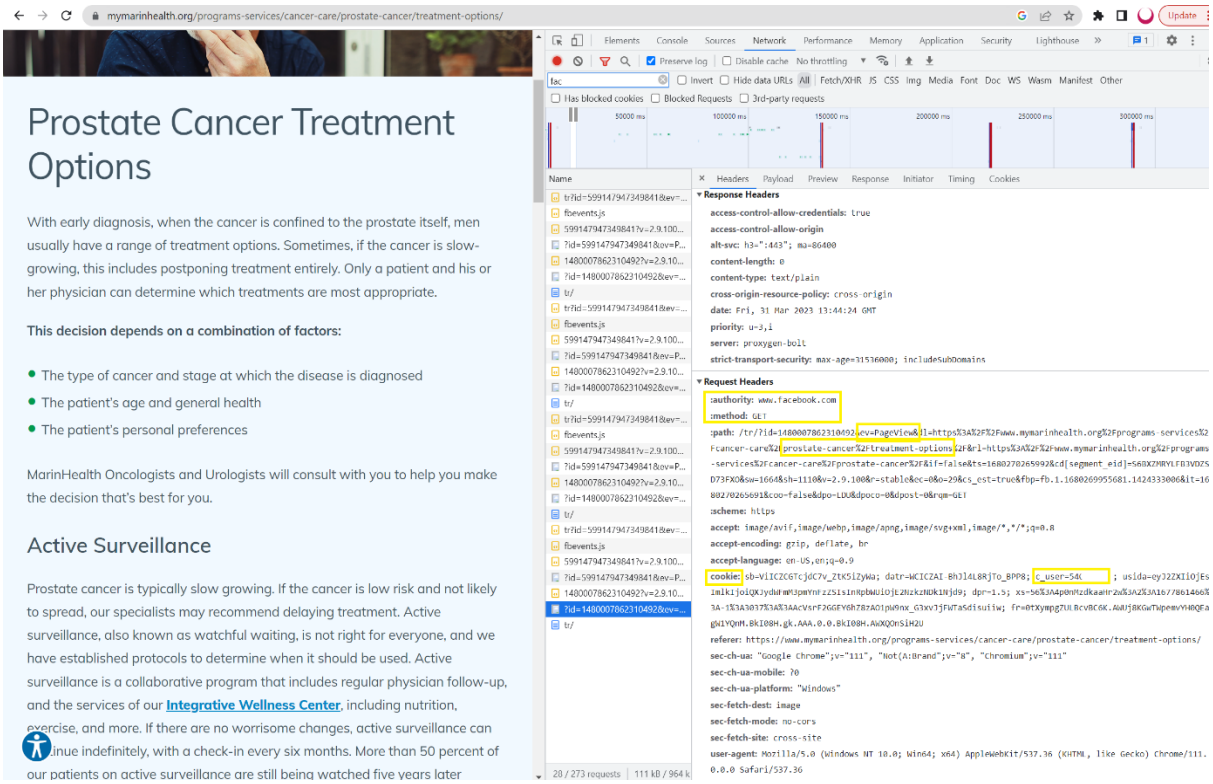
///

///

///

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

***Figure 3**: An HTTP single communication session sent to Facebook that reveals the User's exact search terms ("prostate cancer treatment options") and the User's unique Facebook ID.*[18]



52. In addition to controlling a website's Markup, Source Code executes a host of other programmatic instructions and can command a website visitor's browser to send data transmissions to third parties via Pixels or web bugs,[19] effectively open a spying window through which the webpage can funnel the visitor's data, actions, and communications to third parties.

53. Looking to the previous example, Defendant's Source Code manipulates the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) and sending those communications to Facebook.

54. This occurs because the Pixel embedded in Defendant's Source Code is programmed to automatically track and transmit a patient's communications, and this occurs contemporaneously, invisibly, and without the patient's knowledge.

[18] The image depicted in ***Figure 3*** was taken from https://www.mymarinhealth.org/programs-services/cancer-care/prostate-cancer/treatment-options/.

[19] These Pixels or web bugs are tiny image files that are invisible to website users. They are purposefully designed in this manner, or camouflaged, so that users remain unaware of them.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

55. Thus, without Users' consent, Defendant effectively uses this Source Code to commandeer patients' computing devices, thereby re-directing their Private Information to unauthorized third parties.

56. The information that Defendant's Pixel sends to Facebook may include, among other things, patients' PII, PHI, and other confidential information.

57. Consequently, when Plaintiff and Class Members visit Defendant's Websites and communicate their Private Information, it is transmitted to Facebook, including, but not limited to, patient status, health conditions experienced and treatments sought, physician selected, appointments sought, specific button/menu selections, sensitive demographic information such as sexual orientation, and exact words and phrases typed into the search bar. Additionally, this includes instances when patients pay a bill, self-enroll in the patient portal, or access their portal via a designated button (or link) on the website. Each of these activities involves the transmission of sensitive information—such as payment details, personal identifiers required for portal enrollment, and portal usage data—which is inevitably communicated to Facebook.

Defendant's Pixel Tracking Practices caused Plaintiff's and Class Members' Private Information to be sent to Facebook.

58. Defendant utilizes Facebook's Business Tools and intentionally installs the Pixel and/or CAPI on their Web Properties to secretly track patients by recording their activity and experiences in violation of its common law, contractual, statutory, and regulatory duties, and obligations.

59. Defendant's web pages contain a unique identifier which indicates that the Pixel is being used on a particular webpage.

60. The Pixels allow Defendant to optimize the delivery of advertisements, measure cross-device conversions, create custom audiences, and decrease advertising and marketing costs.

61. However, Defendant's Web Properties do not rely on the Pixel to function.

62. While seeking and using Defendant's services as a medical provider, Plaintiff and Class Members communicated their Private Information to Defendant via their Web Properties.

63. Defendant did not disclose to Plaintiff and Class Members that their Private

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Information would be shared with Facebook as it was communicated to Defendant. Rather, Defendant represented the opposite. This prevents the provision of any informed consent by Plaintiff or Class Members to Defendant for the challenged conduct described herein.

64. Plaintiff and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information to Facebook (or any other third-party), nor did they intend for Facebook to be a party to their communications with Defendant. Defendant did not employ any form or click system whereby Plaintiff and Class Members provide their affirmative consent to Defendant agreeing, authorizing, or otherwise permitting Defendant to disclose their Private Information to Facebook (or any other third-party).

65. Defendant's Pixels and CAPI sent sensitive Private Information to Facebook, including but not limited to Plaintiff's and Class Members': (i) status as medical patients; (ii) health conditions; (iii) sought treatment or therapies; (iv) terms and phrases entered into Defendant's search bar; (v) sought providers and their specialties; (vi) selected locations or facilities for treatment; and (vii) web pages viewed.

66. Importantly, the Private Information Defendant's Pixels sent to Facebook was sent alongside Plaintiff's and Class Members' personal identifiers, including patients' IP address and cookie values thereby allowing individual patients' communications with Defendant, and the Private Information contained in those communications, to be linked to their unique Facebook accounts.

67. Through the Source Code deployed by Defendant, the cookies that they use to help Facebook identify patients include but are not necessarily limited to cookies named: "c_user," "datr," "fr," and "fbp."[20]

68. The "*c_user*" cookie or FID is a type of third-party cookie assigned to each person who has a Facebook account, and it is composed of a unique and persistent set of numbers.

69. A User's FID is linked to their Facebook profile, which generally contains a wide

[20] Defendant's Websites track and transmit data via first-party and third-party cookies. C_user, datr, and fr cookies are third-party cookies. The fbp cookie is a Facebook identifier that is set by Facebook source code and associated with Defendant's use of the Facebook Pixel. The fbp cookie emanates from Defendant's Website as a putative first-party cookie, but is transmitted to Facebook through cookie syncing technology that hacks around the same-origin policy.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

range of demographics and other information about the User, including pictures, personal interests, work history, relationship status, and other details. Because the User's Facebook Profile ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook Profile ID to quickly locate, access, and view the user's corresponding Facebook profile.

70. The "*datr*" cookie identifies the patient's specific web browser from which the patient is sending the communication. It is an identifier that is unique to the patient's specific web browser and is therefore a means of identification for Facebook users. Facebook keeps a record of every datr cookie identifier associated with each of its users, and a Facebook user can obtain a redacted list of all datr cookies associated with his or her Facebook account from Facebook.

71. The "*fr*" cookie is a Facebook identifier that is an encrypted combination of the c_user and datr cookies.[21]

Defendant's Pixel Disseminates Patient Information Via Their Websites.

72. By way of example, if a patient uses https://www.mymarinhealth.org to look for medical treatments, they may select "Gender Affirmation" under the "Programs & Services" tab, which takes them to the list of services offered by Defendant to Users in need of gender affirmation surgery. On those pages the user can further narrow their search results by services offered by Defendant.

73. The User's selections and filters are transmitted to Facebook via the Meta Pixels, even if they contain the User's treatment, procedures, medical conditions, or related queries, without alerting the User, and the images below confirm that the communications Defendant sends to Facebook contain the User's Private Information and personal identifiers, including but not limited to their IP address, Facebook ID, and datr and fr cookies, along with the search filters the User selected.

74. For example, a patient in search for gender affirmation surgery can search for various surgery procedure options, from "top surgery" and "body contouring" to resources intended to help

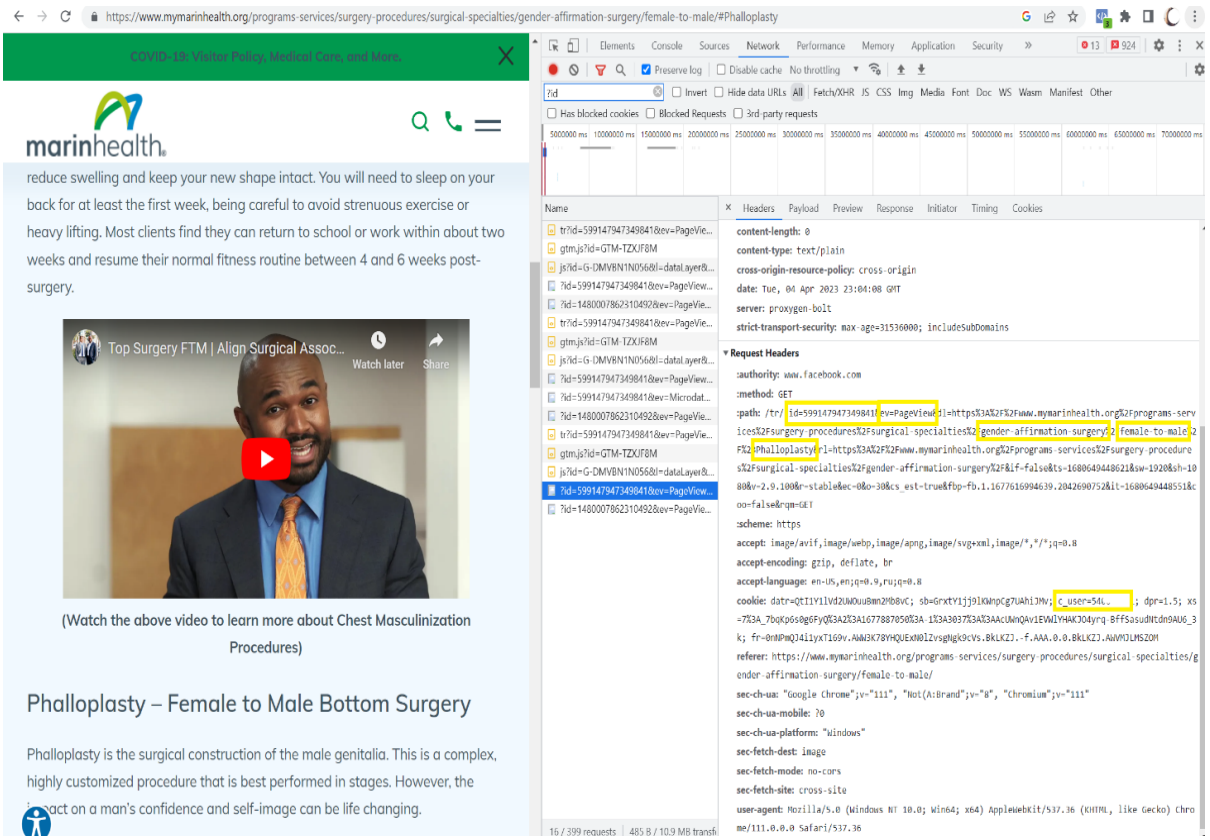
[21] *See* Gunes Acar et al., *Facebook Tracking Through Social Plug-ins: Technical Report prepared for the Belgian Privacy Commission* 16 (March 27, 2015), https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf (last visited Aug. 4, 2023).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

patients navigate their gender identity journey.[22]

75. From the moment the patient begins searching for gender affirmation, their selections or search parameters are automatically transmitted by the Pixel to Facebook along with the User's unique personal identifiers, as evidenced by Figure 4 below.

***Figure 4:** Defendant's transmission to Facebook of User's search parameters showing treatment sought ("phalloplasty") and the User's unique Facebook ID.*



76. The first line of highlighted text, "id = 599147947349841," refers to the Defendant's Pixel ID for this particular Webpage and confirms that the Defendant has downloaded the Pixel into its Source Code on this particular Webpage.

77. In the second line of text, "ev:" is an abbreviation for event, and "PageView" is the type of event. Here, this event means that Defendant's Pixel is sending information about the webpage the User is visiting, which can include information like page title, URL, and page description.

[22] *See Gender Affirmation Surgery,* MARINHEALTH, https://www.mymarinhealth.org/programs-services/surgery-procedures/surgical-specialties/gender-affirmation-surgery/.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

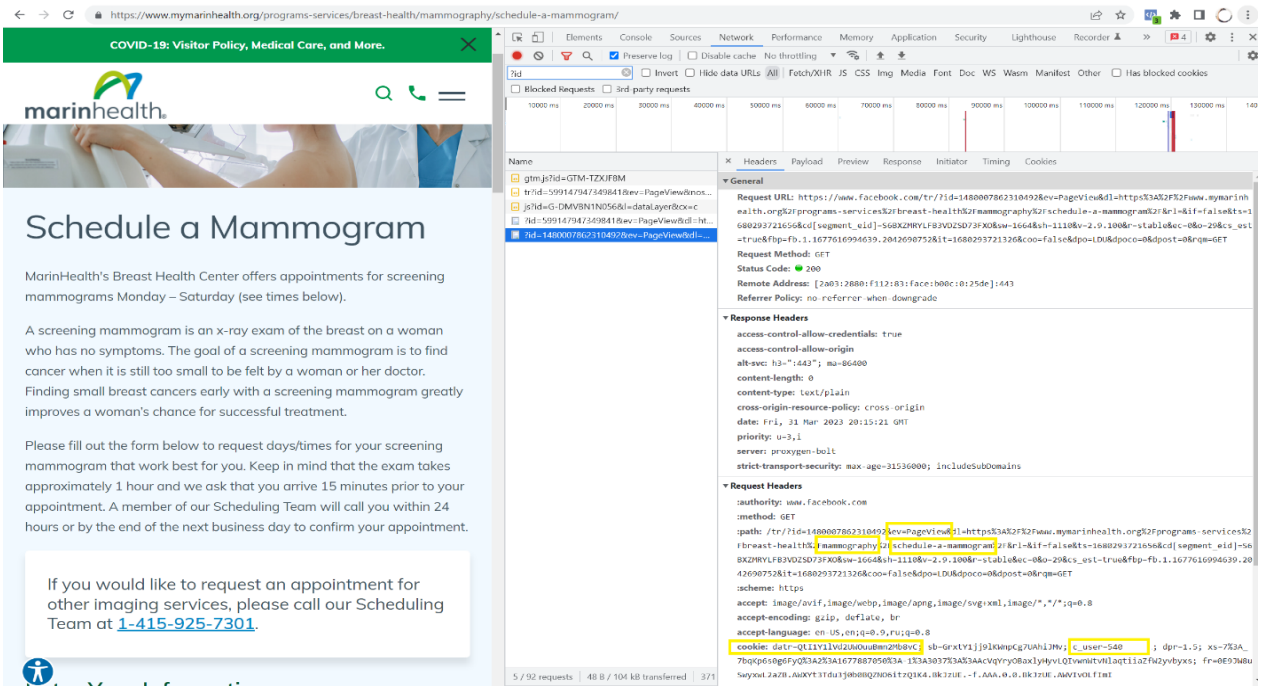
78. The remaining lines of text identify the User as a patient: (i) seeking medical care from Defendant via www.mymarinhealth.org; (ii) who is seeking gender affirmation surgery; and (iii) who is searching for phalloplasty.

79. Finally, the text ("GET"), demonstrates that Defendant's Pixel sent the User's communications, and the Private Information contained therein, alongside the User's personal identifiers, including Facebook ID and other cookies.

80. Defendant offers many types of services and treatments, including options to schedule certain types of treatments, on its Website. For example, under "Breast Health" services, a User can select from various medical services including "Mammogram."

81. This action takes the User to one of Defendant's web pages for mammograms where the User can click on the button "Schedule A Mammogram" and fill out a form to request an appointment. All of this information is being shared with Facebook as well, including if the User clicks the dedicated phone number button to schedule the service:

Figure 5: HTTP communication session sent from the User's device to Facebook revealing the User is trying to schedule an appointment for a mammogram, and their personal identifiers.

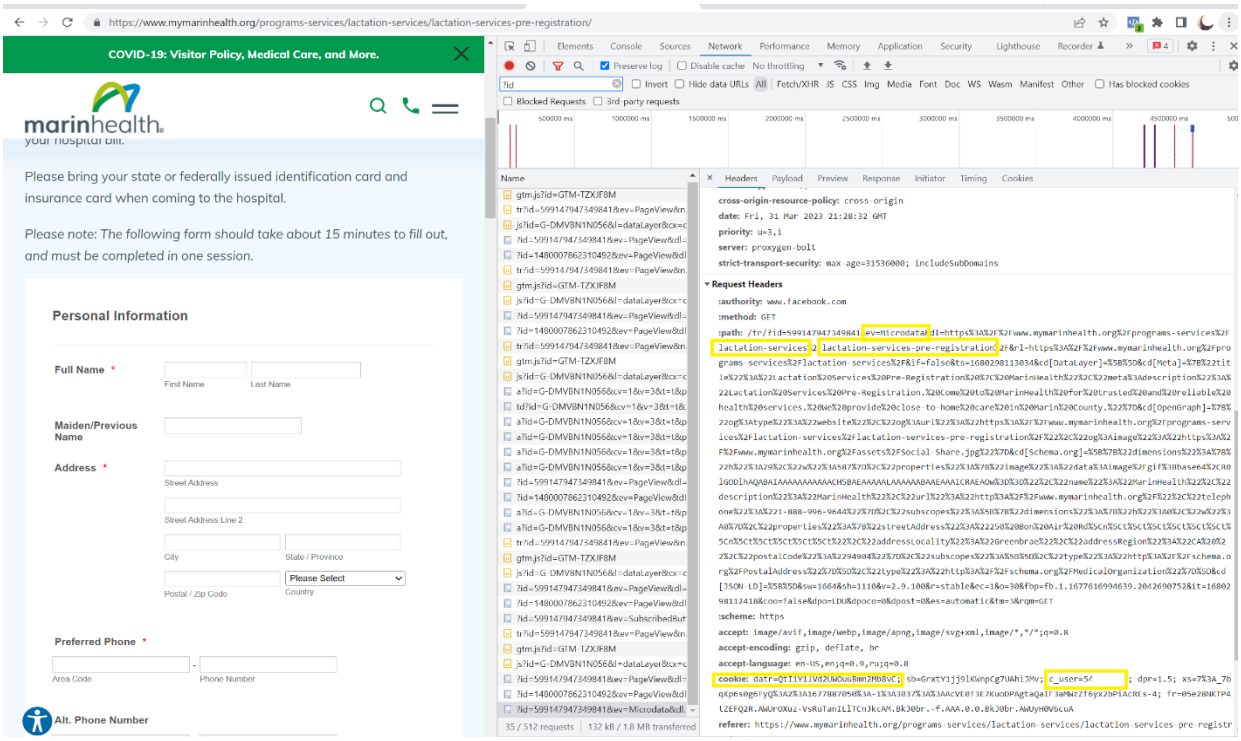


82. By way of another example, among the various services offered as part of its women's care, Defendant offers lactation support to new mothers, including the option to "pre-register" for

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

these services. When a pregnant or new mother in search of lactation services visits these pages, Defendant transmits this information to Facebook:

Figures 6: ***HTTP communication sessions sent from the User's device to Facebook revealing the navigation path by the User interested in lactation services.***



83. Additionally, a patient can use Defendant's website to search for a provider based on their name and/or specialty.

84. These search terms, including those disclosing the User's medical condition or treatment sought, are also transmitted via the Facebook Pixel:

///

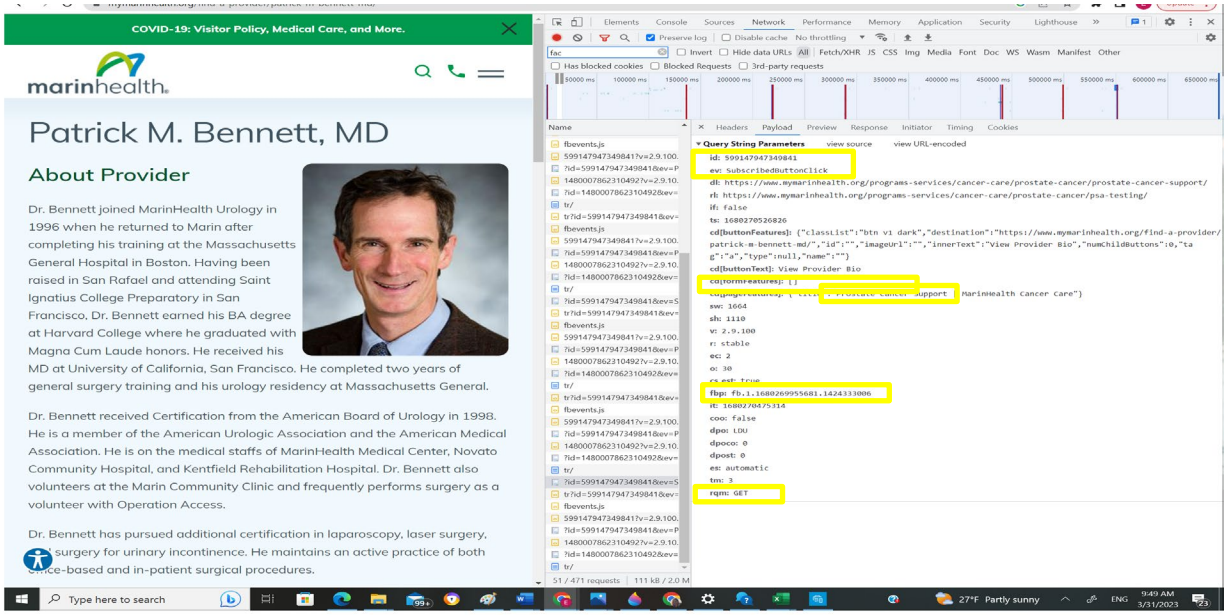
///

///

///

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

***Figure 7*: HTTP communication session sent from the User's device to Facebook disclosing that the User is looking for a prostate cancer specialist and the provider's name.**



85. The Facebook Tracking Pixel uses both first- and third-party cookies. A first-party cookie is "created by the website the user is visiting"—i.e., Defendant.[23]

86. A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"—i.e., Facebook.[24]

87. The _fbp cookie is always transmitted as a first-party cookie. A duplicate _fbp cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

88. Facebook, at a minimum, uses the fr, _fbp, and c_user cookies to link to FIDs and corresponding Facebook profiles.

89. As shown in the figures above, Defendant sent these identifiers with the event data.

90. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information, nor did they authorize any assistance with intercepting their communications.

91. Plaintiff was never provided with any written notice that Defendant disclosed its

[23] *First-Party Cookie*, PCMAG.COM, https://www.pcmag.com/encyclopedia/term/first-party-cookie (last visited Aug. 4, 2023). This is confirmable by using developer tools to inspect a website's cookies and track network activity.

[24] *Third-Party Cookie*, PCMAG.COM, https://www.pcmag.com/encyclopedia/term/third-party-cookie (last visited Aug. 4, 2023). This is also confirmable by tracking network activity.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Website Users' Private Information nor were they provided any means of opting out of such disclosures.

92. Despite this, Defendant knowingly and intentionally disclosed Plaintiff's Private Information to Facebook.

Defendant Violates Their Promises to Users and Patients to Protect Their Confidentiality.

93. Defendant did not have the legal right to use or share Plaintiff's and Class Members' data, as this information is protected by the HIPAA Privacy Rule. The Privacy Rule does not permit the use and disclosure of Private Information to Facebook for use in targeted advertising.[25]

94. Beyond Defendant's legal obligations to protect the confidentiality of individuals' Private Information, Defendant's privacy policies and online representations affirmatively and unequivocally state that any personal information provided to Defendant will remain secure and protected.[26]

95. Further, Defendant represents to Users that they will only disclose Private Information provided to them under certain circumstances, ***none of which apply here***.[27] Defendant's privacy policies does ***not*** permit Defendant to use and disclose Plaintiff's and Class Members' Private Information for marketing purposes.

96. In fact, Defendant acknowledges in their Notice of Privacy Practices that they ". . .will not sell or otherwise provide the information [they] collect to outside third parties for the purpose of direct or indirect mass email marketing."[28]

97. Moreover, Defendant represents that they will disclose Users' PHI when required by law or "in the good-faith belief that such action is necessary to: (i) Cooperate with the investigations of purported unlawful activities and conform to the edicts of the law or comply with legal process served on our company; (ii) Protect and defend the rights or property of our Website and related properties; (iii) Identify persons who may be violating the law, the rights of third parties, or

[25] *See* 45 C.F.R. § 164.502.

[26] *Privacy Policy*, MARINHEALTH, https://www.mymarinhealth.org/privacy-policy/ (last visited Aug. 6, 2023).

[27] *See id.*

[28] *See id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

otherwise misusing our Website or its related properties."[29]

98. Further, Defendant's Privacy Policy represents:

> "We follow generally accepted industry standards to protect the information submitted to us, both during transmission and once we receive it."[30]
>
> "To make sure that your health information is protected in a way that doesn't interfere with your health care, your information can be used and shared:
> - For your treatment and care coordination
> - To pay doctors and hospitals for your health care and help run their businesses
> - With your family, relatives, friends, or others you identify who are involved with your health care or your health care bills, unless you object
> - To make sure doctors give good care and nursing homes are clean and safe
> - To protect the public's health, such as by reporting when the flu is in your area
> - To make required reports to the police, such as reporting gunshot wounds."

99. Upon information and belief, none of these circumstances listed above apply here.

100. Finally, in their privacy policy, Defendant acknowledges that, "[p]roviders and health care insurers who are required to follow this law must comply with your right to...receive a notice that tells you how your health information may be used and shared."[31]

101. Defendant failed to issue a notice that Plaintiff and Class Members' Private Information had been impermissibly disclosed to an unauthorized third party. In fact, Defendant ***never*** disclosed to Plaintiff or Class Members that they shared their sensitive and confidential communications, data, and Private Information with Facebook and other third parties.[32]

---

[29] *See id.*

[30] *See id.*

[31] *See id.*

[32] In contrast to Defendant, in recent months several medical providers which have installed the Meta Pixel on their Web Properties have provided their patients with notices of data breaches caused by the Pixel transmitting PHI to third parties. *See*, *e.g.*, *Cerebral, Inc. Notice of HIPAA Privacy Breach*, https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf (last visited Aug. 4, 2023); Annie Burky, *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies,* FIERCE HEALTHCARE (October 20, 2022), https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3; *Novant Health Notifies*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

102. Defendant has unequivocally failed to adhere to a single promise vis-à-vis their duty to safeguard Private Information of their Users. Defendant has made these privacy policies and commitments available on their websites. Defendant included these privacy policies and commitments to maintain the confidentiality of their Users' sensitive information as terms of their contracts with those Users, including contracts entered with Plaintiff and the Class Members. In these contract terms and other representations to Plaintiff and Class Members and the public, Defendant promised to take specific measures to protect Plaintiff's and Class Members' Private Information, consistent with industry standards and federal and state law. However, they failed to do so.

103. Even non-Facebook users can be individually identified via the information gathered on the Digital Platforms, like an IP address or personal device identifying information. This is precisely the type of information for which HIPAA requires the use of de-identification techniques to protect patient privacy.[33]

104. In fact, in an action currently pending against Facebook related to use of their Pixel on healthcare provider web properties, Facebook explicitly stated it requires Pixel users to "post a prominent notice on every page where the Pixel is embedded and to link from that notice to information about exactly how the Pixel works and what is being collected through it, so it is not invisible."[34] Defendant did not post such a notice.

105. Facebook further stated that "most providers [...] will not be sending [patient information] to Meta because it violates Meta's contracts for them to be doing that."[35]

Patients of Potential Data Privacy Incident, PR NEWSWIRE (August 19, 2022), https://www.prnewswire.com/news-releases/novant-health-notifies-patients-of-potential-data-privacy-incident-301609387.html.

[33] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. DEP'T OF HEALTH AND HUM. SERVICES, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Aug. 4, 2023).

[34] *See* Transcript of the argument on Plaintiff's Motion for Preliminary Injunction in *In re Meta Pixel Healthcare Litig.*, *supra* note 6, at 19:12-18.

[35] *Id.* at 7:20-8:11.

106. Despite a lack of disclosure, Defendant allowed third parties to "listen in" on patients' confidential communications and to intercept and use for advertising purposes the very information they promised to keep private, in order to bolster their profits.

Plaintiff and Class Members Reasonably Believed That Their Confidential Medical Information Would Not Be Shared with Third Parties.

107. Plaintiff and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

108. Indeed, at all times when Plaintiff and Class Members provided their Private Information to Defendant, they each had a reasonable expectation that the information would remain confidential and that Defendant would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

109. Personal data privacy and obtaining consent to share Private Information are material to Plaintiff and Class Members.

110. Plaintiff and Class Members relied to their detriment on Defendant's uniform representations and omissions regarding protection privacy, limited uses, and lack of sharing of their Private Information.

111. Now that their sensitive personal and medical information is in possession of third parties, Plaintiff and Class Members face a constant threat of continued harm – including bombardment of targeted advertisements based on the unauthorized disclosure of their personal data. Collection and sharing of such sensitive information without consent or notice poses a great threat to individuals by subjecting them to the never-ending threat of identity theft, fraud, phishing scams, and harassment

Plaintiff and Class Members Have No Way of Determining Widespread Usage of Invisible Pixels.

112. Plaintiff and Class Members have no idea that Defendant is collecting and utilizing their Private Information, including sensitive medical information, when they engage with Defendant's websites which have Meta Pixels secretively incorporated in the background.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

113. Plaintiff and Class Members do not realize that tracking Pixels exist because they are invisibly embedded within Defendant's web pages that users might interact with.[36] Patients and users of Defendant's websites do not receive any alerts during their uses of Defendant's Web Properties stating that Defendant tracks and share sensitive medical data with Facebook, allowing Facebook and other third parties to subsequently target all users of Defendant's websites for marketing purposes.

114. Plaintiff and Class Members trusted Defendant's websites when inputting sensitive and valuable Private Information. Had Defendant disclosed to Plaintiff and Class Members that every click, every search, and every input of sensitive information was being tracked, recorded, collected, and ***disclosed*** to third parties, Plaintiff and Class Members would not have trusted Defendant's websites to input such sensitive information.

115. Defendant knew or should have known that Plaintiff and Class Members would reasonably rely on and trust Defendant's promises regarding the tracking privacy and uses of their Private Information. Furthermore, any person visiting a health website has a reasonable understanding that medical providers must adhere to strict confidentiality protocols and are bound not to share any medical information without their consent.

116. By collecting and sharing Users' Private Information with Facebook and other unauthorized third parties, Defendant caused harm to Plaintiff, Class Members, and all affected individuals.

117. Furthermore, once Private Information is shared with Facebook, such information may not be effectively removed, even though it includes personal and private information.

118. Plaintiff fell victim to Defendant's unlawful collection and sharing of their sensitive medical information using the Meta Pixel tracking code on their websites.

///

///

///

[36] FTC Office of Technology, *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, FED. TRADE COMM'N (March 16, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Facebook Use of Tracking Pixels in Advertising Business.

119. Facebook is one of the largest advertising companies in the country, with over 2.9 billion active users.[37]

120. Realizing the value of having direct access to millions of consumers, in 2007, Facebook began monetizing its platform by launching "Facebook Ads," proclaiming it to be a "completely new way of advertising online" that would allow "advertisers to deliver more tailored and relevant ads."[38]

121. Given the highly specific data used to target specific users, it is no surprise that millions of companies and individuals utilize Facebook's advertising services. Meta generates almost all of its revenue from selling advertisement placements:

Year	Total Revenue	Ad Revenue	% Ad Revenue
2023 Q1	$28.65 billion	$28.101 billion	98.1%
2022	$116.61 billion	$113.64 billion	97.5%
2021	$117.93 billion	$114.93 billion	97.46%
2020	$85.97 billion	$84.17 billion	97.90%
2019	$70.70 billion	$69.66 billion	98.52%
2018	$55.84 billion	$55.01 billion	98.51%

122. One of its most powerful advertising tools is Meta Pixel, formerly known as Facebook Pixel, which launched in 2015.

123. Ad Targeting has been extremely successful due, in large part, to Facebook's ability to target people at a granular level. "Among many possible target audiences, Facebook offers advertisers, [for example,] 1.5 million people 'whose activity on Facebook suggests that they're more likely to engage with/distribute liberal political content' and nearly seven million Facebook users who 'prefer high-value goods in Mexico.'"[39]

124. Acknowledging that micro-level targeting is highly problematic, in November of 2021 Facebook announced that it was removing options that "relate to topics people may perceive

[37] S. Dixon, *Facebook Users by Country 2023*, STATISTA (February 24, 2023), www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/.

[38] *Facebook Unveils Facebook Ads*, META (November 6, 2007), https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/.

[39] Natasha Singer, *What You Don't Know about How Facebook Uses Your Data*, N.Y. TIMES (April 11, 2018), https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

as sensitive," such as "Health causes (e.g., 'Lung cancer awareness', 'World Diabetes Day', 'Chemotherapy'), Sexual orientation (e.g., 'same-sex marriage' and 'LGBT culture')", "Religious practices and groups (e.g., 'Catholic Church' and 'Jewish holidays')," as well as "Political beliefs, social issues, causes, organizations, and figures."

125. For Facebook, the Pixel acts as a conduit of information, sending the information it collects to Facebook through scripts running in the User's internet browser. The information is sent in data packets labeled with PII, including the User's IP address.

126. If the User has a Facebook account, the Private Information collected is linked to the individual Users' Facebook account. For example, if the User is logged into their Facebook account when the User visits a website where the Meta Pixel is installed, many common browsers will attach third-party cookies allowing Facebook to link the data collected by the Pixel to the specific Facebook user.

127. Alternatively, Facebook can link the data to a users' Facebook account through the "Facebook Cookie." The Facebook Cookie is a workaround to recent cookie-blocking techniques, including one developed by Apple, Inc., to track users.[40]

128. Facebook can also link Private Information to Facebook accounts through identifying information collected via Meta Pixel through what Facebook calls "Advanced Matching."[41] There are two forms of Advanced Matching: manual matching and automatic matching. Using Manual Advanced Matching the website developer manually sends data to Facebook to link users. Using Automatic Advanced Matching, the Pixel scours the data it receives to search for recognizable fields, including name and email address to match users to their Facebook accounts.[42]

129. A recent investigation revealed that the Meta Pixel was installed inside password-protected patient portals of at least seven health systems.[43] When a User navigates through their

[40] Maciej Zawadziński & Michal Wlosik, *What Facebook's First-Party Cookie Means for AdTech,* CLEAR CODE (June 8, 2022), https://clearcode.cc/blog/facebook-first-party-cookie-adtech/.

[41] Illia Lahunou, *What is Advanced Matching in Facebook Pixel and How it Works,* VERFACTO, https://www.verfacto.com/blog/ecommerce/advanced-matching-facebook-pixel/ (last visited Aug. 4, 2023); *see also About advanced matching for web*, META, https://www.facebook.com/business/help/611774685654668?id=1205376682832142 (last visited Aug. 4, 2023).

[42] *Id.*

[43] *See* Feathers, *et al*., *supra* note 3.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

patient portal, the Meta Pixel sends Facebook sensitive data including but not limited to, the User's medication information, prescriptions, descriptions of their issues, notes, test results, and details about upcoming doctor's appointments.

130. David Holtzman, a health privacy consultant was "deeply troubled" by the results of The Markup's investigation and indicated "it is quite likely a HIPAA violation" by the hospitals, such as Defendant.[44]

131. Laura Lazaro Cabrera, a legal officer at Privacy International, indicated that Facebook's access to use even only some of these data points—such as just the URL—is problematic. She explained, "Think about what you can learn from a URL that says something about scheduling an abortion' . . . 'Facebook is in the business of developing algorithms. They know what sorts of information can act as a proxy for personal data."[45]

132. When Users visit websites that have incorporated the Meta Pixel, the Pixel collects information about Users' activity on that website. This information is then shared with Facebook and, in tandem with data from the Users' Facebook profile such as their age, gender, and interests, can be used to target the user with advertisements on Facebook and other websites that use the Pixel.

133. However, the collection and use of this data raises concerns about user privacy and the potential misuse of personal information. For example, when Users browse Defendant's Web Properties, every bit of their activity is tracked and monitored. By analyzing this data using algorithms and machine learning techniques, these entities tracking this information can learn a chilling level of detail about Users' behavioral patterns, preferences, and interests.

134. While this data can be used to provide personalized and targeted content and advertising, it can also be used for more nefarious purposes, such as tracking and surveillance. For example, if an advertiser or social media platform has access to a User's browsing history, search queries, and social media activity, they could potentially build a detailed profile of that User's behavior patterns, including where they go, what they do, and who they interact with.

---

[44] *Id.*

[45] Grace Oldham & Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients*, THE MARKUP (Aug. 4, 2022), https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

135. This level of surveillance and monitoring raises important ethical and legal questions about privacy, consent, and the use of personal data. It is important for Users to be aware of how their data is being collected and used, and to have control over how their information is shared and used by advertisers and other entities.

136. Moreover, the misuse of this data could potentially lead to the spread of false or misleading information, which could have serious consequences, particularly in the case of health-related information. As an example, the Cambridge Analytica scandal revealed that personal data was misused to target individuals with political propaganda and misinformation.[46]

137. The Cambridge Analytica scandal involved the misuse of personal data collected from Facebook users, which was then used to target individuals with political advertising and propaganda. The scandal highlighted the potential dangers of using personal data for targeted advertising and the need for greater transparency and accountability in the collection and use of personal information.[47] One of the ways that Cambridge Analytica was able to collect personal data was through the use of third-party apps that collected data from users and their friends. This data was then used to build detailed profiles of individuals, which were used to target them with personalized political ads and propaganda.

138. The use of algorithms and machine learning techniques to analyze this data allowed Cambridge Analytica to identify patterns in users' behavior and preferences, which were then used to target them with specific messages and ads.

139. This highlights the potential dangers of using personal data to build detailed profiles of individuals, particularly when that data is collected without their knowledge or consent. It also raises important questions about the ethics of using personal data for political purposes and the need for greater regulation and oversight of data collection and use.

140. Finally, as pointed out by the OCR, impermissible disclosures of such data in the healthcare context "may result in identity theft, financial loss, discrimination, stigma, mental

[46] Sam Meredith, *Here's Everything You Need to Know about the Cambridge Analytica Scandal*, CNBC (March 23, 2018), https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html.

[47] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI…. This tracking information could also be misused to promote misinformation, identity theft, stalking, and harassment."[48]

141. In conclusion, as Judge Orrick pointed out in a recent decision allowing claims under California and common law against Regents of the University of California for collecting personal medical data via the Meta Pixel to go forward, "[p]ersonal medical information is understood to be among the most sensitive information that could be collected about a person" and unauthorized transmission or interception of such data by third parties may constitute a "highly offensive" intrusion of privacy. *Doe v. Regents of Univ. of Cal.*, 23-cv-00598-WHO (N.D. Cal. May 6, 2023).

Defendant Knew Plaintiff's Private Information Included Sensitive Medical Information, Including Medical Records.

142. Defendant was aware that by incorporating the Meta Pixel onto their websites, this would result in the disclosure and use of Plaintiff's and Class Members' Private Information, including sensitive medical information.

143. By virtue of how the Meta Pixel works, i.e., sending all interactions on a website to Facebook, Defendant was aware that their Users' Private Information would be sent to Facebook when they researched specific medical conditions and/or treatments, looked up providers, made appointments, typed specific medical queries into the search bar, and otherwise interacted with Defendant's Web Properties.

144. Indeed, software companies like MyChart that provide online access to medical records utilized by Defendant have "specifically recommended heightened caution around the use of custom analytics." Despite this, Defendant continued to use the Meta Pixel on their Web Properties.

///

///

///

[48] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, supra* note 12.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Plaintiff and Class Members Have a Reasonable Expectation of Privacy in Their Private Information, Especially with Respect to Sensitive Medical Information.

145. Plaintiff and Class Members have a reasonable expectation of privacy in their Private Information, including personal information and sensitive medical information.

146. Patient PHI specifically is protected by federal law under HIPAA.

147. HIPAA sets national standards for safeguarding protected health information. For example, HIPAA limits the permissible uses of health information and prohibits the disclosure of this information without explicit authorization. *See* 45 C.F.R. § 164.502. HIPAA also requires that covered entities implement appropriate safeguards to protect this information. *See* 45 C.F.R. § 164.530(c)(1).

148. This federal legal framework applies to health care providers, including Defendant.

149. Given the application of HIPAA to the Defendant, Plaintiff and the members of the Class had a reasonable expectation of privacy over their PHI.

150. Several studies examining the collection and disclosure of consumers' sensitive medical information confirm that the collection and unauthorized disclosure of sensitive medical information from millions of individuals, as Defendant has done here, violates expectations of privacy that have been established as general societal norms.

151. Privacy polls and studies uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

152. For example, a recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

them.[49] Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.[50]

153. Users act consistent with these preferences. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85% of worldwide users and 94% of U.S. users chose not to share data when prompted.[51]

154. Medical data is particularly even more valuable because unlike other personal information, such as credit card numbers which can be quickly changed, medical data is static. This is why companies possessing medical information, like Defendant, are intended targets of cyber-criminals.[52]

155. Patients using Defendant's Web Properties must be able to trust that the information they input including their physicians, their health conditions and courses of treatment will be protected. Indeed, numerous state and federal laws require this. And these laws are especially important when protecting individuals with medical conditions such as HIV or AIDS that can and do subject them to regular discrimination. Furthermore, millions of Americans keep their health information private because it can become the cause of ridicule and discrimination. For instance, despite the anti-discrimination laws, persons living with HIV/AIDS are routinely subject to discrimination in healthcare, employment, and housing.[53]

[49] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/.

[50] *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CENTER (November 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[51] Margaret Taylor, *How Apple Screwed Facebook*, WIRED (May 19, 2021), https://www.wired.co.uk/article/apple-ios14-facebook.

[52] Caroline Humer & Jim Finkle, *Your medical record is worth more to hackers than your credit card*, REUTERS (September 24, 2014), https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924.

[53] Bebe J. Anderson, JD, *HIV Stigma and Discrimination Persist, Even in Health Care*, AMA J. ETHICS (December 2009), https://journalofethics.ama-assn.org/article/hiv-stigma-and-discrimination-persist-even-health-care/2009-12.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

156. The concern about sharing medical information is compounded by the reality that advertisers view this type of information as particularly high value. Indeed, having access to the data women share with their healthcare providers allows advertisers to obtain data on children before they are even born. As one article put it: "the datafication of family life can begin from the moment in which a parent thinks about having a baby."[54] The article continues, "[c]hildren today are the very first generation of citizens to be datafied from before birth, and we cannot foresee — as yet — the social and political consequences of this historical transformation. What is particularly worrying about this process of datafication of children is that companies like . . . Facebook . . . are harnessing and collecting multiple typologies of children's data and have the potential to store a plurality of data traces under unique ID profiles."[55]

157. Other privacy law experts have expressed concerns about the disclosure to third parties of a users' sensitive medical information. For example, Dena Mendelsohn—the former Senior Policy Counsel at Consumer Reports and current Director of Health Policy and Data Governance at Elektra Labs—explained that having your personal health information disseminated in ways you are unaware of could have serious repercussions, including affecting your ability to obtain life insurance and how much you pay for that coverage, increase the rate you are charged on loans, and leave you vulnerable to workplace discrimination.[56]

158. Defendant surreptitiously collected and used Plaintiff's and Class Members' Private Information, including highly sensitive medical information, through Meta Pixel in violation of Plaintiff's and Class Members' privacy interests.

///

///

///

///

[54] Veronica Barassi, *Tech Companies Are Profiling Us From Before Birth*, MIT PRESS READER (January 14, 2021), https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth/.

[55] *Id.*

[56] Class Action Complaint, *Jane Doe v. Regents of the Univ. of Cal. d/b/a UCSF Medical Center*, CLASS ACTION (Feb. 9, 2023), https://www.classaction.org/media/doe-v-regents-of-the-university-of-california.pdf.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

REPRESENTATIVE PLAINTIFF'S EXPERIENCE

Plaintiff C.M.:

159. Plaintiff has a rare autoimmune condition and has been a patient at MarinHealth Medical Center in Greenbrae, California for many years. Plaintiff started using the MarinHealth website over three years ago, utilizing the Patient Portal many times in the recent years. Plaintiff has had a Facebook account for over a decade, and suddenly started to receive unsolicited advertisements relating to his medical conditions shortly after visiting MarinHealth's Properties.

160. Defendant encouraged Plaintiff to utilize MarinHealth's website and online portal in order to search for doctors, make appointments, review medical treatments, and to review charts from previous exams.[57]

161. While using Defendant's Web Properties, Plaintiff communicated sensitive – and what he expected to be confidential – personal and medical information to Defendant.

162. Plaintiff used MarinHealth's Web Properties to research healthcare providers (including specialists and primary care providers) and communicate with them, research particular medical conditions (such as his rare autoimmune disease) and treatments, fill out forms and questionnaires, schedule and attend appointments, and perform other tasks related to his specific medical inquiries and treatment.

163. Plaintiff also utilized MarinHealth's Patient Portal to refill prescriptions, look at his bills and payments, to see his test results and notes from his appointments and from his visits to the ER.

164. While using MarinHealth's digital services, Plaintiff communicated and received information regarding his appointments, treatments, medications, and clinical information,

[57] *See, e.g.*, *MyChart – MarinHealth's Patient Portal* MARINHEALTH, https://www.mymarinhealth.org/mychart/ ("MarinHealth Medical Center and MarinHealth Medical Network Clinics are on a single medical record system. This powerful technology creates a seamless experience throughout your entire health journey, whether you are being seen in a clinic or at the hospital. Your providers can immediately access all of your health information in one place, so they can more informed decisions about your diagnosis and treatment plan, resulting in more coordinated care. As part of this medical record system, you'll have access to your health information in **MyChart**, our patient portal. You can complete pre-visit tasks, view test results, medication lists, upcoming appointments, medical bills, price estimates, and more all in one place using the app on your phone or computer").

including his surgeries, ER visits, lab work, and scans. As a result of the Meta Pixel Defendant chose to install on their Web Properties, this information was intercepted, viewed analyzed, and used by unauthorized third parties.

165. Plaintiff accessed MarinHealth's Web Properties in connection with receiving healthcare services from MarinHealth or MarinHealth's affiliates at MarinHealth's direction and with MarinHealth's encouragement.

166. Plaintiff has used and continues to use the same devices to maintain and to access an active Facebook account throughout the relevant period in this case.

167. As a medical patient using MarinHealth's health services, Plaintiff reasonably expected that his online communications with MarinHealth were solely between himself and MarinHealth, and that such communications would not be transmitted or intercepted by a third party. Plaintiff also relied on MarinHealth's Privacy Policies in reasonably expecting MarinHealth would safeguard his Private Information. But for his status as MarinHealth's patient and its representations via their Privacy Policies, Plaintiff would not have disclosed his Private Information to MarinHealth.

168. Plaintiff is also an active Facebook user and has had a Facebook account since at least 2008.

TOLLING, CONCEALMENT & ESTOPPEL

169. The applicable statutes of limitation have been tolled as a result of Defendant's knowing and active concealment and denial of the facts alleged herein.

170. Defendant secretly incorporated the Meta Pixel into its Web Properties and patient portals, providing no indication to Users that their User Data, including their Private Information, would be disclosed to unauthorized third parties.

171. Defendant had exclusive knowledge that the Meta Pixel was incorporated on its Web Properties, yet failed to disclose that fact to Users, or inform them that by interacting with their websites Plaintiff's and Class Members' User Data, including Private Information, would be disclosed to third parties, including Facebook.

172. Plaintiff and Class Members could not with due diligence have discovered the full scope of Defendant's conduct because the incorporation of Meta Pixels is highly technical and there

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

were no disclosures or other indications that would inform a reasonable consumer that Defendant was disclosing and allowing Facebook to intercept Users' Private Information.

173. The earliest Plaintiff and Class Members could have known about Defendant's conduct was shortly before the filing of this Complaint.

174. As alleged above, Defendant has a duty to disclose the nature and significance of their data disclosure practices but failed to do so. Defendant is therefore estopped from relying on any statute of limitations under the discovery rule.

CLASS ALLEGATIONS

175. **Class Definition:** Plaintiff brings this action on behalf of themself and on behalf of various classes of persons similarly situated, as defined below, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.:

176. The Nationwide Class that Plaintiff seeks to represent is defined as:

> **Nationwide Class**: All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the Meta Pixel on Defendant's Web Properties.

177. The California Subclass that Plaintiff seeks to represent is defined as:

> **California Subclass:** All individuals residing in the State of California whose Private Information was disclosed to a third party without authorization or consent through the Meta Pixel on Defendant's Web Properties.

178. The Nationwide Class, and the California Subclass are referred to collectively as the "Classes." Excluded from the Classes are Defendant, their agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant's officer or director, any successor or assign and any Judge who adjudicates this case, including their staff and immediate family.

179. **The following people are excluded from the Classes:** (1) any Judge or Magistrate presiding over this action and members of their immediate families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or their parents have a controlling interest and its current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

180. Plaintiff reserves the right under Federal Rule of Civil Procedure 23 to amend or modify the Classes to include a broader scope, greater specificity, further division into subclasses, or limitations to particular issues. Plaintiff reserves the right under Federal Rule of Civil Procedure 23(c)(4) to seek certification of particular issues.

181. The requirements of Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3) are met in this case.

182. The Fed. R. Civ. P. 23(a) elements of Numerosity, Commonality, Typicality, and Adequacy are all satisfied.

183. **Numerosity:** The exact number of Class Members is not available to Plaintiff, but it is clear that individual joinder is impracticable. Hundreds of thousands of people have used MarinHealth's Web Properties since at least 2015. Members of the Class can be identified through Defendant's records or by other means.

184. **Commonality:** Commonality requires that the Class Members' claims depend upon a common contention such that determination of its truth or falsity will resolve an issue that is central to the validity of each claim in one stroke. Here, there is a common contention for all Class Members as to whether Defendant disclosed to third parties their Private Information without authorization or lawful authority.

185. **Typicality:** Plaintiff's claims are typical of the claims of other Class Members in that Plaintiff and the Class Members sustained damages arising out of Defendant's uniform wrongful conduct and data sharing practices.

186. **Adequate Representation:** Plaintiff will fairly and adequately represent and protect the interests of the Class Members. Plaintiff's claims are made in a representative capacity on behalf of the Class Members. Plaintiff has no interests antagonistic to the interests of the other Class Members. Plaintiff has retained competent counsel to prosecute the case on behalf of Plaintiff and

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

the Class. Plaintiff and Plaintiff's counsel are committed to vigorously prosecuting this action on behalf of the Class members.

187. The declaratory and injunctive relief sought in this case includes, but is not limited to:

a. Entering a declaratory judgment against Defendant—declaring that Defendant's interception of Plaintiff's and Class Members' Private Information among themselves and other third parties is in violation of the law;

b. Entering an injunction against Defendant:

i. preventing Defendant from sharing Plaintiff's and Class Members' Private Information among themselves and other third parties;

ii. requiring Defendant to alert and/or otherwise notify all users of its websites and portals of what information is being collected, used, and shared;

iii. requiring Defendant to provide clear information regarding their practices concerning data collection from the users/patients of Defendant's Web Properties, as well as uses of such data;

iv. requiring Defendant to establish protocols intended to remove all personal information which has been leaked to Facebook and/or other third parties, and request Facebook/third parties to remove such information;

v. and requiring Defendant to provide an opt out procedure for individuals who do not wish for their information to be tracked while interacting with Defendant's Web Properties.

188. **Predominance:** There are many questions of law and fact common to the claims of Plaintiff and Class Members, and those questions predominate over any questions that may affect individual Class Members. Common questions and/or issues for Class members include, but are not necessarily limited to the following:

i. Whether Defendant's acts and practices violated California's Constitution, Art. 1, § 1;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

ii. Whether Defendant's acts and practices violated California's Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq.*;

iii. Whether Defendant's acts and practices violated the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*;

iv. Whether Defendant's unauthorized disclosure of Users' Private Information was negligent;

v. Whether Defendant owed a duty to Plaintiff's and Class Members not to disclose their Private Information to unauthorized third parties;

vi. Whether Defendant breached their duty to Plaintiff's and Class Members not to disclose their Private Information to unauthorized third parties;

vii. Whether Defendant represented to Plaintiff and the Class that they would protect Plaintiff's and the Class Members' Private Information;

viii. Whether Defendant violated Plaintiff's and Class Members' privacy rights;

ix. Whether Defendant's practices violated California's Confidentiality of Medical Information Act, Civ. Code §§ 56, *et seq.*;

x. Whether Defendant's practices violated California's Constitution, Art. 1, § 1;

xi. Whether Plaintiff and Class Members are entitled to actual damages, enhanced damages, statutory damages, and other monetary remedies provided by equity and law;

xii. Whether injunctive and declaratory relief, restitution, disgorgement, and other equitable relief is warranted.

189. **Superiority:** This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by individual Class Members will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual Class Members to obtain effective relief from Defendant's misconduct. Even if Class Members could mount such individual litigation, it would still not be

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single Court. Economies of time, effort and expense will be enhanced, and uniformity of decisions ensured.

190. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant misrepresented that it would disclose personal information only for limited purposes that did not include purposes of delivering advertisements or collecting data for commercial use or supplementing consumer profiles created by data aggregators and advertisers;

b. Whether Defendant's privacy policies misrepresented that it collected and shared User information with third-party service providers only for the limited purpose of providing access to its services;

c. Whether Defendant misrepresented that it had in place contractual and technical protections that limit third-party use of User information and that it would seek User consent prior to sharing Private Information with third parties for purposes other than provision of its services;

d. Whether Defendant misrepresented that any information it receives is stored under the same guidelines as any health entity that is subject to the strict patient data sharing and protection practices set forth in the regulations propounded under HIPAA;

e. Whether Defendant misrepresented that it complied with HIPAA's requirements for protecting and handling Users' PHI;

f. Whether Defendant shared the Private Information that Users provided to Defendant with advertising platforms, including Facebook, without adequate

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

notification or disclosure, and without Users' consent, in violation of health privacy laws and rules and its own privacy policy;

g. Whether Defendant integrated third-party tracking tools, consisting of automated web beacons ("**Pixels**") in its websites that shared Private Information and User activities with third parties for unrestricted purposes, which included advertising, data analytics, and other commercial purposes;

h. Whether Defendant shared Private Information and activity information with Facebook using Facebook's tracking Pixels on its websites without Users' consent;

i. Whether Facebook used the information that Defendant shared with it for unrestricted purposes, such as selling targeted advertisements, data analytics, and other commercial purposes.

COUNT ONE

VIOLATION OF THE CONFIDENTIALITY OF MEDICAL INFORMATION ACT CAL. CIV. CODE §§ 56, *et seq.*

(On behalf of Plaintiff and the California Subclass against Defendant)

191. Plaintiff incorporates paragraphs and herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

192. Defendant is subject to the CMIA pursuant to California Civil Code § 56.10 because they are a "provider of health care" as defined by California Civil Code § 56.06(b); they operate hospitals, provide health care, maintain medical information, offer software to consumers designed to maintain medical information for the purposes of communications with doctors, receipt of diagnosis, treatment, or management of medical conditions.

193. Section 56.10 states, in pertinent part, that "[n]o provider of health care . . . shall disclose medical information regarding a patient of the provider of health care . . . without first obtaining an authorization . . . ."

194. Section 56.101 of the CMIA states, in pertinent part, that "[a]ny provider of health care . . . who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

medical information shall be subject to the remedies and penalties . . .” Cal. Civ. Code §§ 56.10, 56.101.

195. Plaintiff’s and California Subclass Members’ Private Information constitutes “medical information” under the CMIA because it consists of individually identifiable information in possession of and derived from a provider of healthcare regarding Plaintiff’s and California Subclass Members’ medical history, test results, mental or physical condition, and/or treatment.

196. Defendant violated Cal. Civ. Code § 56.10 because it failed to maintain the confidentiality of Users’ medical information, and instead “disclose[d] medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization” by soliciting, intercepting, and receiving Plaintiff’s and California Subclass Members’ Private Information, and sharing it with advertisers and for advertising purposes. Specifically, Defendant knowingly, willfully, or negligently disclosed Plaintiff’s and California Subclass Members’ medical information to Facebook, allowing Facebook to now advertise and target Plaintiff and California Subclass Members, misusing their extremely sensitive Private Information.

197. Defendant violated Cal. Civ. Code § 56.101 because it knowingly, willfully, or negligently failed to create, maintain, preserve, store, abandon, destroy, and dispose of medical information in a manner that preserved its confidentiality by soliciting, intercepting, and receiving Plaintiff’s and California Subclass Members’ Private Information, and sharing it with advertisers and for advertising purposes for Facebook’s and Defendant’s financial gain.

198. Defendant intentionally embedded Facebook Pixels, which facilitates the unauthorized sharing of Plaintiff’s and California Subclass Members’ medical information.

199. Defendant violated Cal Civ. Code § 56.36(b) because it negligently released confidential information and records concerning Plaintiff and California Subclass Members in violation of their rights under the CMIA.

200. As a direct and proximate result of Defendant’s misconduct, Plaintiff and California Subclass Members had their private communications containing information related to their sensitive and confidential Private Information intercepted, disclosed, and used by third parties.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

201. As a result of Defendant's unlawful conduct, Plaintiff and California Subclass Members suffered an injury, including violation to their rights of privacy, loss of the privacy of their Private Information, loss of control over their sensitive personal information, and suffered aggravation, inconvenience, and emotional distress.

202. Plaintiff and California Subclass Members are entitled to: (a) nominal damages of $1,000 per violation; (b) actual damages, in an amount to be determined at trial; (c) reasonable attorneys' fees, and costs.

COUNT TWO

VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ("CIPA"), CAL. PENAL CODE § 630, *et seq.*

(On behalf of Plaintiff and the California Subclass against Defendant)

203. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

204. Defendant is a person for purposes of Cal. Penal Code §631.

205. CIPA § 631(a) imposes liability for "distinct and mutually independent patterns of conduct." *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to establish liability under CIPA § 631(a), a plaintiff need only establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner," does any of the following: (1) "intentionally taps, or makes any unauthorized connection…with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system," (2) "willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within [the state of California]," (3) "uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained," or (4) ***aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section***" (emphasis added).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

206. Section 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' Internet browsing history).

207. Defendant's Web Properties are a "machine, instrument, contrivance, or ... other manner" used to engage in the prohibited conduct at issue here.

208. At all relevant times, Defendant entered into contracts with Facebook, in order to track certain activities on its Web Properties. Defendant allowed Facebook to intercept and otherwise track Users' clicks, communications, searches, and other User activities. Defendant and activated Facebook Pixel tracking tools, allowing Facebook to intentionally tap, and make unauthorized connections with, the lines of internet communication between Plaintiff and California Subclass Members on the one hand, and Defendant's Web Properties on the other hand, without consent of all parties to the communication.

209. At all relevant times, by using the Facebook Pixel, Facebook willfully and without the consent of Plaintiff and California Subclass Members, read or attempted to learn the contents or meaning of electronic communications of Plaintiff and putative California Subclass Members on Defendant's Web Properties. This occurred while the electronic communications were in transit or passing over any wire, line, or cable, or were being sent from or received at any place within California. Facebook intercepted Plaintiff's and California Subclass Members' communications – including the very terms and phrases they typed into the search bar – without their authorization or consent.

210. By embedding Facebook Pixels on their websites, Defendant aided, agreed with, employed, and conspired with Facebook to wiretap consumers communications on Defendant's

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Web Properties using the Facebook Pixel snipped codes and to accomplish the wrongful conduct at issue here.

211. Plaintiff and California Subclass Members did not consent to the interception, reading, learning, recording, and collection of their electronic communications with Defendant. Accordingly, the interception was unlawful and tortious.

212. The violation of section 631(a) constitutes an invasion of privacy sufficient to confer Article III standing.

213. Unless enjoined, Defendant will continue to commit the illegal acts alleged here. Plaintiff continues to be at risk because he frequently uses Defendant's Web Properties to search for information about medical products, health conditions or services. Plaintiff continues to desire to use the Defendant's Web Properties for that purpose, including but not limited to investigating health conditions (e.g., diabetes), diagnoses (e.g., COVID-19), procedures, test results, treatment status, the treating physician, medications, and/or allergies.

214. Plaintiff and California Subclass Members may or are likely to visit Defendant's Web Properties in the future but have no practical way of knowing whether their website communications will be collected, viewed, accessed, stored, and used by Facebook.

215. Plaintiff and California Subclass Members seek all relief available under Cal. Penal Code § 637.2, including injunctive relief and statutory damages of $5,000 per violation.

COUNT THREE

VIOLATION OF THE UNFAIR COMPETITION LAW ("UCL")

CALIFORNIA BUSINESS AND PROFESSIONS CODE § 17200, *et seq.*

(On behalf of Plaintiff and the Nationwide Class against Defendant)

216. Plaintiff herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

A. Unlawful Prong

217. Defendant's conduct as alleged herein was unfair within the meaning of the UCL. The unfair prong of the UCL prohibits unfair business practices that either offend an established public

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

policy or that are immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers.

218. Defendant's conduct, as alleged herein, was also fraudulent within the meaning of the UCL. Defendant made deceptive misrepresentations and omitted known material facts in connection with the solicitation, interception, disclosure, and use of Plaintiff's and Nationwide Class Members' Private Information. Defendant actively concealed and continued to assert misleading statements regarding their protection and limitation on the use of the Private Information. Meanwhile, Defendant was collecting and sharing Plaintiff's and Nationwide Class Members' Private Information without their authorization or knowledge to profit off of the information and deliver targeted advertisements to Plaintiff and Nationwide Class Members, among other unlawful purposes.

219. Defendant's conduct, as alleged herein, was unlawful within the meaning of the UCL because they violated regulations and laws as discussed herein, including but not limited to HIPAA, Section 5 of the Federal Trade Commission Act ("**FTCA**"), 15 U.S.C. § 45, and the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et seq*.

220. Had Plaintiff and Nationwide Class Members known Defendant would disclose and misuse their Private Information in contravention of Defendant's representations, they would never have used Defendant's website or their MyChart portal and would not have shared their Private Information.

221. Defendant's unlawful actions in violation of the UCL have caused and are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.

222. As a direct and proximate result of Defendant's misconduct, Plaintiff and Nationwide Class Members had their private communications containing information related to their sensitive and confidential Private Information intercepted, disclosed, and used by third parties, including but not limited to Facebook.

223. As a result of Defendant's unlawful conduct, Plaintiff and Nationwide Class Members suffered an injury, including violation to their rights of privacy, loss of value and privacy of their

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Private Information, loss of control over their sensitive personal information, and suffered embarrassment and emotional distress as a result of this unauthorized sharing of information.

B. Unfair Prong

224. Defendant engaged in unfair business practices by disclosing Plaintiff's and Nationwide Class Members' Private Information to unrelated third parties, including Facebook, without prior consent despite their promises to keep such information confidential.

225. Defendant's unfair business practices included widespread violations of Plaintiff's and Nationwide Class Members' rights to privacy, including their failure to inform the public that using their Web Properties would result in disclosure of highly private information to third parties.

226. Because Defendant is in the business of providing medical and mental healthcare services, Plaintiff and Nationwide Class Members relied on Defendant to advise them of any potential disclosure of their Private Information.

227. Plaintiff and Nationwide Class Members were entitled to assume, and did assume, that Defendant would take appropriate measures to keep their Private Information secure and confidential. At no point did Plaintiff expect to become a commodity on which Defendant and Facebook would trade.

228. Plaintiff and Nationwide Class Members reasonably relied upon the representations Defendant made in their Privacy Policy, including those representations concerning the confidentiality of Private Information, such as patient health information.

229. Defendant was in sole possession of and had a duty to disclose the material information that Plaintiff and Nationwide Class Members' private information was being shared with third parties.

230. Had Defendant disclosed that it shared Private Information with third parties, Plaintiff and the Nationwide Class would not have used Defendant's services at the level they did.

231. The harm caused by the Defendant's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendant's legitimate business interests other than Defendant's conduct described herein.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

232. Defendant's acts, omissions and conduct also violate the unfair prong of the UCL because those acts, omissions and conduct offended public policy (including the aforementioned federal and state privacy statutes and state consumer protection statutes, such as HIPAA), and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff and Nationwide Class Members.

233. As a direct result of Plaintiff's and Nationwide Class Members' reliance on Defendant's representations that Defendant would keep their Private Information confidential and Defendant's express representation that they would not share Private Information with third parties without the Users' express consent, Plaintiff and Nationwide Class Members shared highly sensitive information through their use of the Web Properties, causing them to suffer damages when Defendant disclosed said information to a third party.

234. As a direct result of Defendant's violations of the UCL, Plaintiff and Nationwide Class Members have suffered injury in fact and lost money or property, including but not limited to payments to Defendant and/or other valuable consideration. The unauthorized access to Plaintiff's and Nationwide Class Members' private and personal data also diminished the value of that Private Information.

235. As a direct result of its unfair practices, Defendant has been unjustly enriched and should be required to make restitution to Plaintiff and Nationwide Class Members pursuant to §§ 17203 and 17204 of the California Business & Professions Code, disgorgement of all profits accruing to Defendant because of their unlawful business practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civ. Proc. §1021.5) and injunctive or other equitable relief.

COUNT FOUR

INVASION OF PRIVACY UNDER CALIFORNIA CONSTITUTION, ART. I, § 1.

(On behalf of Plaintiff and the California Subclass

against Defendant)

236. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

237. Art. I, § 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const., Art. I, § 1.

238. The right to privacy in California's Constitution creates a private right of action against private and government entities.

239. Plaintiff and California Subclass Members have and continue to have a reasonable expectation of privacy and interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential communications and protected health information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to wiretaps without their knowledge, authorization, or consent.

240. At all relevant times, by using Facebook's Meta Pixel to record and communicate patients' FIDs and other individually identifying information alongside their confidential medical communications, Defendant invaded Plaintiff's and California Subclass Members' privacy rights under the California Constitution.

241. Plaintiff and California Subclass Members had a reasonable expectation that their communications, identity, health information, and other data would remain confidential, and that the Defendant would not install wiretaps on their Web Properties to secretly transmit communications to a third party.

242. Plaintiff and California Subclass Members did not authorize the Defendant to record and transmit their Private Information – including private medical communications alongside their personally identifiable health information – to a third party, Facebook. *See* Figures 2-9 of Defendant's Web Properties above.

243. This invasion of privacy is serious in nature, scope, and impact because it relates to patients' private medical communications. Moreover, it constitutes an egregious breach of the societal norms underlying the privacy right.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

244. As a result of the Defendant's actions, Plaintiff and California Subclass Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

245. Plaintiff and California Subclass Members have been damaged as a direct and proximate result of the Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

246. Plaintiff and California Subclass Members seek appropriate relief for their injuries, including but not limited to damages that will reasonably compensate Plaintiff and California Subclass Members for the harm to their privacy interests as a result of the intrusion(s) upon Plaintiff's and California Subclass Members' privacy.

247. Plaintiff and California Subclass Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of the Defendant's conduct, injuring Plaintiff and California Subclass Members in conscious disregard of their rights.

248. Plaintiff seeks all other relief as the Court may deem just, proper, and available for invasion of privacy under the California Constitution, on behalf of the California Subclass.

COUNT FIVE

INVASION OF PRIVACY

INTRUSION UPON SECLUSION

(On behalf Plaintiff and the Nationwide Class against Defendant)

249. Plaintiff herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

250. Plaintiff and Nationwide Class Members had a reasonable and legitimate expectation of privacy in the Private Information that Defendant failed to adequately protect against disclosure from unauthorized parties.

251. Defendant owed a duty to Plaintiff and Nationwide Class Members to keep their Private Information confidential.

252. Defendant failed to protect, and instead released to unknown and unauthorized third parties, the Private Information of Plaintiff and Nationwide Class Members.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

253. By failing to keep Plaintiff's and Nationwide Class Members' Private Information confidential and safe from misuse, Defendant knowingly shared highly sensitive Private Information with Facebook, Defendant unlawfully invaded Plaintiff's and Nationwide Class Members' privacy by, among others: (i) intruding into Plaintiff's and Nationwide Class Members' private affairs in a manner that would be highly offensive to a reasonable person; (ii) failing to adequately secure their Private Information from disclosure to unauthorized persons; and (iii) enabling and facilitating the disclosure of Plaintiff's and Class Members' Private Information without authorization or consent.

254. Plaintiff's and Nationwide Class Members' expectation of privacy was and is especially heightened given Defendant's consistent representations that Users' information would remain confidential and would not be disclosed to anyone without User consent.

255. Defendant's privacy policy specifically provides, "We will not sell or otherwise provide the information we collect to outside third parties for the purpose of direct or indirect mass email marketing."[58]

256. Defendant knew, or acted with reckless disregard of the fact that a reasonable person in Plaintiff's and Nationwide Class Members' position would consider their actions highly offensive.

257. Defendant's unauthorized surreptitious recording, monitoring, and sharing of the Users' activities, searches, researching diagnosis and treatment, searching for doctors and medical specialists violated expectations of privacy that have been established by social norms.

258. As a proximate result of such unauthorized disclosures, Plaintiff's and Nationwide Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted and caused damages to Plaintiff and Nationwide Class Members.

259. Plaintiff and Nationwide Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's conduct, directed at injuring Plaintiff and Nationwide Class Members in conscious disregard of their rights.

[58] *Notice of Privacy Policy*, *supra* note 42.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

260. Plaintiff seeks injunctive relief on behalf of the Nationwide Class, restitution, as well as any and all other relief that may be available at law or equity. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause irreparable injury to Plaintiff and Nationwide Class Members. Plaintiff and Nationwide Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Nationwide Class.

COUNT SIX

NEGLIGENCE

(On behalf Plaintiff and the Nationwide Class against Defendant)

261. Plaintiff herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

262. Defendant owed a duty to Plaintiff and the Nationwide Class to exercise due care in collecting, storing, safeguarding, and preventing any disclosure of their Private Information. This duty included but was not limited to: (a) preventing Plaintiff's and Nationwide Class Members' Private Information from being to be disclosed to unauthorized third parties; and (b) destroying Plaintiff's and Nationwide Class Members' Private Information within an appropriate amount of time after it was no longer required by Defendant.

263. Defendant's duties to use reasonable care arose from several sources, including those described below. Defendant had a common law duty to prevent foreseeable harm to others, including Plaintiff and Nationwide Class Members, who were the foreseeable and probable victims of any data misuse, such as disclosure of Private Information to unauthorized parties.

264. Defendant had a special relationship with Plaintiff and Nationwide Class Members, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Nationwide Class Members resulting from unauthorized disclosure of their Private Information to third parties such as Facebook. Plaintiff and Nationwide Class Members were compelled to entrust Defendant with their Private Information. At relevant times, Plaintiff and Nationwide Class Members understood that Defendant would take adequate

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

data storage practices to safely store their Private Information. Only Defendant had the ability to protect Plaintiff's and Nationwide Class Members' Private Information collected and stored on Defendant's websites.

265. Defendant's duty to use reasonable measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of [PHI]." 45 C.F.R. § 164.530(c)(1).

266. Defendant's conduct as described above constituted an unlawful breach of their duty to exercise due care in collecting, storing, and safeguarding Plaintiff's and the Nationwide Class Members' Private Information by failing to protect this information.

267. Plaintiff and Nationwide Class Members trusted Defendant and in doing so provided Defendant with their Private Information, based upon Defendant's representations that they would "follow generally accepted industry standards to protect the information submitted to [them], both during transmission and once [they] receive it."[59] Defendant failed to do so.

268. Defendant breached their duty in this relationship to collect and safely store Plaintiff's and Nationwide Class Members' Private Information.

269. Plaintiff's and the Nationwide Class Members' Private Information would have remained private and secure had it not been for Defendant's wrongful and negligent breach of their duties. Defendant's negligence was, at least, a substantial factor in causing Plaintiff's and Nationwide Class Members' Private Information to be improperly accessed, disclosed, and otherwise compromised, and in causing Plaintiff and the Nationwide Class Members other injuries because of the unauthorized disclosures.

270. The damages suffered by Plaintiff and the Nationwide Class Members were the direct and reasonably foreseeable result of Defendant's negligent breach of their duties to maintain Users' Private Information. Defendant knew or should have known that their unauthorized disclosure of highly sensitive Private Information was a breach of their duty to collect and safely store such information.

[59] *Privacy Policy*, *supra* note 42.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

271. Defendant's negligence directly caused significant harm to Plaintiff and the Nationwide Class. Specifically, Plaintiff and Nationwide Class Members are now subject to their sensitive information being accessed by unauthorized parties, which may lead to significant harms.

272. Plaintiff hereby incorporates all other paragraphs as if fully stated herein.

273. Defendant had a fiduciary duty to protect the confidentiality of their communications with Plaintiff and Nationwide Class Members by virtue of the explicit privacy representations Defendant made on their websites to Plaintiff and members of the Nationwide Class.

274. Defendant had information relating to Plaintiff and Nationwide Class Members that they knew or should have known to be confidential.

275. Plaintiff's and Nationwide Class Members' communications with Defendant about sensitive Private Information and their status as patients of Defendant were not matters of general knowledge.

276. Defendant breached their fiduciary duty of confidentiality by designing their data protection systems in a way to allow for a data breach of a massive caliber.

277. At no time did Plaintiff or Nationwide Class Members give informed consent to Defendant's conduct.

278. As a direct and proximate cause of Defendant's actions, Plaintiff and Nationwide Class Members suffered damage in that the information they intended to remain private is no longer so and their Private Information was disclosed to, tracked, and intercepted by third-party Internet tracking companies, including Facebook, without their knowledge or consent.

COUNT SEVEN

BREACH OF IMPLIED CONTRACT

(On behalf of Plaintiff and the Nationwide Class against Defendant)

279. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Nationwide Class.

280. When Plaintiff and Nationwide Class Members provided their Private Information to Defendant in exchange for services, they entered into implied contracts by which Defendant agreed to safeguard and not disclose such Private Information without consent.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

281. Plaintiff and Nationwide Class Members accepted Defendant's offers of services and provided their Private Information to Defendant via the Web Properties.

282. Plaintiff and Nationwide Class Members would not have entrusted Defendant with their Private Information in the absence of an implied contract between them that included Defendant's promise not to disclose Private Information without consent.

283. Defendant breached these implied contracts by disclosing Plaintiff's and Nationwide Class Members' Private Information to third parties, including Facebook.

284. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiff and Nationwide Class Members sustained damages as alleged herein. Plaintiff and Nationwide Class Members would not have used Defendant's services, or would have paid substantially less for these services, had they known their Private Information would be disclosed.

285. Plaintiff and Nationwide Class Members are entitled to compensatory and consequential damages as a result of Defendant's breach of implied contract.

COUNT EIGHT

LARCENY/RECEIPT OF STOLEN PROPERTY (VIOLATION OF CALIFORNIA PENAL CODE § 496(a) and (c))

(On behalf of Plaintiff and the California Subclass against Defendant)

286. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed California Subclass.

287. Courts recognize that internet users have a property interest in their personal information and data. *See Calhoun v. Google, LLC,* 526 F. Supp. 3d 605, at *21 (N.D. Cal. Mar. 17, 2021) (recognizing property interest in personal information and rejecting Google's argument that "the personal information that Google allegedly stole is not property"); *In re Experian Data Breach Litigation,* 2016 U.S. Dist. LEXIS 184500, at *5 (C.D. Cal. Dec. 29, 2016) (loss of value of PII is a viable damages theory); *In re Marriott Int'l Inc. Customer Data Sec. Breach Litig.,* 440 F. Supp. 3d 447, 460 (D. Md. 2020) ("The growing trend across courts that have considered this issue is to

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

recognize the lost property value of this [personal] information."); *Simona Opris v. Sincera,* 2022 U.S. Dist. LEXIS 94192, at *20 (E.D. Pa. 2022) (collecting cases).

288. Cal. Penal Code §496(c) permits "any" person who has been injured by a violation of section 496(a) to recover three times the amount of actual damages, costs of suit and attorney's fees in a civil suit.

289. Penal Code § 496(a) creates an action against "any" person who (1) receives "any" property that has been stolen or obtained in any manner constituting theft, knowing the property to be stolen or obtained, or (2) conceals, sells, withholds, or aids in concealing or withholding "any" property from the owner, knowing the property to be so stolen or illegally obtained.

290. Under Penal Code § 1.07(a)(38), "person" means "an individual, corporation, or association." Thus, Defendant is a person under section 496(a).

291. As set forth herein, the Users' Private Information was stolen or obtained by theft, without limitation, under Penal Code §484, by false or fraudulent representations or pretenses. At no point did the Defendant have Plaintiff's and California Subclass Members' consent to duplicate their searches and send them to Facebook.

292. Defendant meets the grounds for liability of section 496(a) because they, and each of them:

a. knew the Private Information was stolen or obtained by theft and/or false pretenses; and, with such knowledge,

b. transmitted such information to unauthorized third parties, like Facebook.

293. Defendant violated the second ground for liability of section 496(a) because they, and each of them:

a. knew the Private Information was stolen or obtained by theft; and, with such knowledge,

b. concealed, withheld, or aided in concealing or withholding said data from their rightful owners by unlawfully tracking the data and disclosing it to unauthorized third parties, like Facebook.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

294. As a direct and proximate result of the acts and omissions described above, Plaintiff and California Subclass Members were injured by the Defendant's violations of section 496(a).

295. Pursuant to California Penal Code § 496(c), the Plaintiff and California Subclass Members seek actual damages, treble damages, costs of suit, and reasonable attorneys' fees.

COUNT NINE

UNJUST ENRICHMENT

(On behalf of Plaintiff and Nationwide Class against Defendant)

296. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

297. By virtue of the unlawful, unfair and deceptive conduct alleged herein, Defendant knowingly realized hundreds of millions of dollars in revenue from the use of the Private Information of Plaintiff and Classes Members for profit by way of targeted advertising related to Users' respective medical conditions and treatments sought.

298. This Private Information, the value of the Private Information, and/or the attendant revenue, were monetary benefits conferred upon Defendant by Plaintiff and Class Members.

299. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in the loss of value of their Private Information and the lost profits from the use of their Private Information.

300. It would be inequitable and unjust to permit Defendant to retain the enormous economic benefits (financial and otherwise) it has obtained from and/or at the expense of Plaintiff and Class Members.

301. Defendant will be unjustly enriched if they are permitted to retain the economic benefits conferred upon them by Plaintiff and Class Members through Defendant's obtaining the Private Information and the value thereof, and profiting from the unlawful, unauthorized, and impermissible use of the Private Information of Plaintiff and Class Members.

302. Plaintiff and Class Members are therefore entitled to recover the amounts realized by Defendant at the expense of Plaintiff and Class Members.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

303. Plaintiff and the Class Members have no adequate remedy at law and are therefore entitled to restitution, disgorgement, and/or the imposition of a constructive trust to recover the amount of Defendant's ill-gotten gains, and/or other sums as may be just and equitable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of himself and the Proposed Classes defined herein, respectfully requests:

A. That this Action be maintained as a Class Action, that Plaintiff be named as Class Representative of the Class, that the undersigned be named as Lead Class Counsel of the Class, and that notice of this Action be given to Class Members;

B. That the Court enter an order:

a. Preventing Defendant from sharing Plaintiff's and Class Members' Private Information among themselves and other third parties;

b. Requiring Defendant to alert and/or otherwise notify all users of its websites and portals of what information is being collected, used, and shared;

c. Requiring Defendant to provide clear information regarding its practices concerning data collection from the users/patients of Defendant's Web Properties, as well as uses of such data;

d. Requiring Defendant to establish protocols intended to remove all personal information which has been leaked to Facebook and/or other third parties, and request Facebook/third parties to remove such information;

e. Requiring Defendant to provide an opt out procedures for individuals who do not wish for their information to be tracked while interacting with Defendant's Web Properties;

f. Mandating the proper notice be sent to all affected individuals, and posted publicly;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

g. Requiring Defendant to delete, destroy, and purge the Private Information of Users unless Defendant can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Users;

h. Requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

C. That the Court award Plaintiff and the Class Members damages (both actual damages for economic and non-economic harm and statutory damages) in an amount to be determined at trial;

D. That the Court issue appropriate equitable and any other relief (including monetary damages, restitution, and/or disgorgement) against Defendant to which Plaintiff and the Class are entitled, including but not limited to restitution and an Order requiring Defendant to cooperate and financially support civil and/or criminal asset recovery efforts;

E. Plaintiff and the Class be awarded with pre- and post-judgment interest (including pursuant to statutory rates of interest set under State law);

F. Plaintiff and the Class be awarded with the reasonable attorneys' fees and costs of suit incurred by their attorneys;

G. Plaintiff and the Class be awarded with treble and/or punitive damages insofar as they are allowed by applicable laws; and

///

///

///

///

///

///

///

///

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

H. Any and all other such relief as the Court may deem just and proper under the circumstances.

JURY TRIAL DEMANDED

Plaintiff demands a jury trial on all triable issues.

DATED: August 16, 2023

CLARKSON LAW FIRM, P.C.

/s/ Yana Hart
Ryan Clarkson, Esq.
Yana Hart, Esq.
Tiara Avaness, Esq.
Valter Malkhasyan, Esq.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com